Mit Stellenmarkt

iX

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

4 April 2008 € 5,50 H 10554

Tutorial, Teil 2:
Samba
in der Windows-Domäne

IT-Security:
Netz-Steganografie
Programmfehler voraussagen

Ebay, Facebook & Co.:
Web 2.0 richtig nutzen
Das WWW als API-Füllhorn

Webprogrammierung:
Anwenderfreundliche Captchas

Mingle:
Agiles Projektmanagement

Embedded Systems:
Mini-DBMS Derby 10.4

Dokumentenmanagement:
Papierloser Landtag

Verteilte Softwareentwicklung:
Subversion 1.5
Eclipse Process Framework

64 Threads parallel:
Suns Niagara 2

Marktübersicht:
Rechner remote nutzen



April 2008
www.ix.de
iX Magazin für professionelle Informationstechnik
Österreich € 6,20 Schweiz CHF 10,70 Benelux € 6,70 Italien € 6,70
Heise
4 199148 505501 04

Von innen zu sehen

SSL, Zertifikate, Smartcards, IPSec – an Sicherheitstechnik herrscht kein Mangel. Wer dem neumodischen Kram nicht traut, kann immer noch den guten alten Safe bemühen. Schade nur, dass weder aktuelle Informationstechnik noch klassische Schlösser helfen, sobald genügend Geld im Spiel ist.

Gut zu beobachten war das an den Vorgängen um den öffentlich hingerichteten ehemaligen Chef der Post und die DVD mit den Kontodaten einiger Hundert deutscher Steuersünder. Für Geld gibt's letztlich alles. Sicher, ein weniger altmodisches Geldinstitut hätte vielleicht die Inhalte seiner Datenbank verschlüsselt – aber was hätte das geholfen? Irgendwann muss irgendwer irgendwo immer auf die unverschlüsselten Daten gucken. Und ob er die nun abschreibt oder mit seiner Handy-Kamera vom Bildschirm abfotografiert oder den Screenshot per Mail verschickt, herausschaffen lässt sich Vertrauliches immer, gegebenenfalls mit viel Aufwand. Vorausgesetzt, die Kasse stimmt.

Unter diesem Gesichtspunkt lohnt sich der Blick auf die Versprechungen im Zusammenhang mit der Gesundheitskarte. Auf ihr selbst werden glücklicherweise kaum relevante Daten gespeichert. Allerdings soll sie als Schlüssel für die Patienten- und die Fallakte gelten. Sie können – nach Zustimmung des Patienten – vom Röntgenbild über den Befund einer psychischen Störung bis zum Ergebnis des HIV-Tests vielerlei enthalten. Und so manches davon dürfte Versicherungen ebenso wie zukünftige Arbeitgeber interessieren. Zentrale Server sollen die Informationen verwalten und somit die gesamten verfügbaren Gesundheitsdaten eines Menschen von überall schnell zugänglich machen. Auf dem mickrigen Chip der Gesundheitskarte wäre ohnehin kein Platz dafür.

Zwar werden die Informationen verschlüsselt. Und sicherlich muss sie ein Arzt auch ohne Zuhilfenahme der Karte des Patienten entschlüsseln können. Denn der liegt womöglich schon längst im Koma oder hat schlicht seine Smartcard nicht mit in den Urlaub genommen. Damit steht prinzipiell dem Diebstahl der Diagnosen nichts mehr im Weg. Vorausgesetzt, die Kasse stimmt.

Da sich der Datenklau durch Insider technisch nicht ausschließen, sondern nur erschweren lässt, bleibt nur, möglichst wenig zu speichern. Für Steuersünder heißt das, nicht mehr zu sündigen. Für alle anderen: Röntgenbilder, Arztbriefe et cetera weiterhin selber auf Papier aufbewahren. Zumal das Gesundheitsministerium bislang noch verspricht, zum Schutz der Daten diene die Verschlüsselung mit dem „geheimen Schlüssel“ des Versicherten. Was die Vermutung nahelegt, zum Dekodieren diene der frei zugängliche öffentliche Schlüssel. Das wäre dann arg viel Technik für gar keinen Schutz.

Christian Kirsch

CHRISTIAN KIRSCH



April 2008

MARKT + TRENDS

TITEL

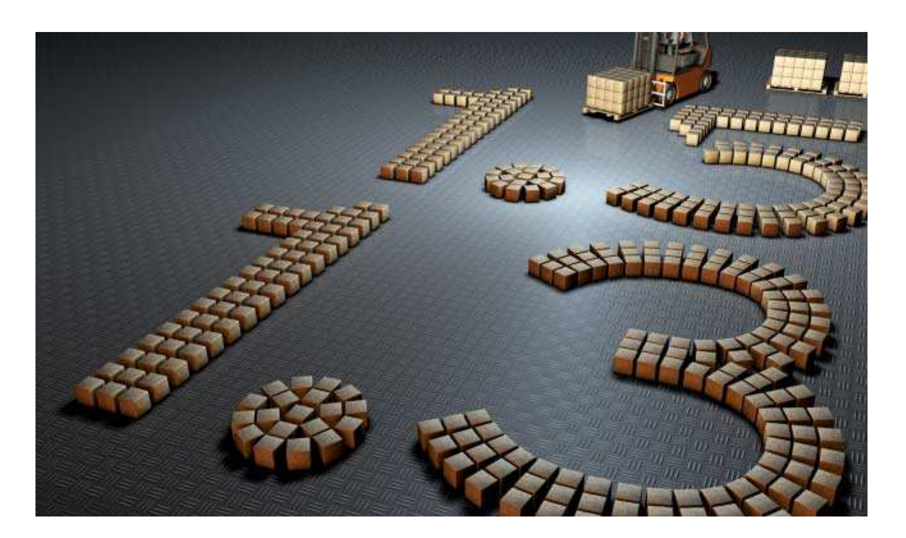
REVIEW



Kontrolle aus der Ferne

Administratoren ganzer Systemlandschaften wie Nutzer einzelner Rechner wollen immer und überall auf ihre Arbeitsumgebung zugreifen können. Das reicht vom einfachen Synchronisieren über gesicherte Zugänge zum System bis hin zum Büro im Netz, in dem Anbieter passende Software-Stacks zur Verfügung stellen. Eine Marktübersicht ab

Seite 106



Verteiltes Subversion

Als Nachfolger von CVS, dem Concurrent Versions System, konnte Subversion in den letzten Jahren „Karriere“ machen. Mit Version 1.5 hat das Versionsverwaltungswerkzeug endlich den überkommenen Zentralismus abgeschüttelt und unterstützt auch verteilte Softwareentwicklung.

Seite 84

Digitale Steiermark

Vom papierlosen Büro träumt die IT seit 20 Jahren – nicht in allen Fällen vergeblich. Denn im Landtag Steiermark erfolgt der Schriftverkehr schon seit 2005 nur noch in elektronischer Form – mit großem Erfolg. Andere Parlamente wie der Landtag Brandenburg planen mittlerweile Ähnliches.

Seite 123





Web 2.0 richtig nutzen

Die Interaktivität des Web 2.0 macht die öffentlichen Programmierschnittstellen der großen Websites erst richtig attraktiv. Zum Stand der Dinge und dem exemplarischen Zugriff auf Ebay und Facebook siehe die

Seiten 66, 72 und 78



Versteckte Übertragung

Dass man Informationen in Bilddateien verstecken kann, ist fast schon ein alter Hut. Aber Header von IP-Paketen lassen sich ebenfalls für die Übermittlung von (geheimen) Zusatzinformationen nutzen. Wie das geht, zeigt der Artikel ab

Seite 112

Gesamtrechenleistung ist entscheidend

(SMP-Server: Tigerton vs. Barcelona – Server mit Intels und AMDs Quad-Core-CPUs; *iX* 3/08; S. 86)

Mit großem Interesse habe ich ihren Artikel gelesen. Aufgefallen ist mir aber die Grafik zur Skalierung auf Seite 88, dort ist der Balken vom Opteron 2350 mit 0,74 kürzer als 0,45 von Intel, aber auch länger als 0,43. Ich glaube, hier liegt ein Fehler vor. Ein anderer Punkt ist, dass ich zur Zeit im Rahmen meiner wissenschaftlichen Arbeit Rechnungen auf unserem Uni-Cluster mit Opteron 2218 durchführe. Da nun neue Maschinen mit Intel Xenon E5345 zur Verfügung stehen, war meine Vorfreude groß. Leider zeigte sich jedoch, dass sobald man 6 der zur Verfügung stehenden 8 Kerne nutzt, die Leistung pro Kern unter der vom Opteron liegt. Ich habe natürlich jeweils möglichst gut für die jeweilige CPU optimiert. Einen solchen Leistungsabfall konnte ich bei den Opterons nicht erkennen. Ich kann nicht wirklich nachvollziehen, warum auf das Thema Skalierung so wenig eingegangen wird und ich lesen kann:

„… AMD mit dem Opteron die bessere Skalierung für sich verbuchen kann, Intel die derzeit höhere Rechenleistung der Cores.“

Zählt denn nicht die höhere Rechenleistung eines Cores, wenn auch die anderen genutzt werden? Man wird ja schließlich keine 8-Kern-Maschine anschaffen, um nur 4 davon zu nutzen, oder? Entscheidend ist doch, wieviel Gesamtrechenleistung bekomme ich pro Maschine.

NILS HUNTEMANN, KASSEL

Konfiguration nur für Fehlersuche

(Samba-Tutorial I: Freier CIFS-Server als Standalone-System; *iX* 3/08; S. 142)

In Ihrem Tutorial zu Samba schlägt die Beraterin vor, den Parameter für die maximale Logfile-Größe auf 0 (unendlich) zu setzen, weil man so nur in einer Datei suchen müsse. Da die von der Autorin vorgeschlagene Konfiguration ja den Sinn hat, Fehlermeldungen nicht durch „wegscrollen“ zu verlieren, man die Datei also auch nicht durch andere Systemmittel abräumen darf, kann dies zum Vollaufen der zugehörigen Partition führen, was je nach Konfiguration mehr oder minder schwere Folgen haben kann. Da sich der Artikel in seiner Form vor allem an Anfänger, interessierte Laien oder Quereinsteiger richtet, möchte ich Sie und oder die Autorin bitten, in der nächsten Ausgabe auf Folgendes hinzuweisen:

Die von der Autorin vorgeschlagene Konfiguration kann bei entsprechender Frequentierung des Servers und/oder entsprechender Laufzeit des Servers durch das Logfile zum Vollaufen der dazugehörigen Partition führen. (Achtung: Die Datei wird auch bei Neustart des Services oder Servers nicht abgeräumt.) Es sei also darauf hingewiesen, dass solcherlei konfigurierte Systeme tatsächlich einer regelmäßigen Überprüfung bedürfen, auch/gerade solange sie keine Probleme machen.

DER DIREKTE DRAHT ZU iX

Redaktion iX
Postfach 61 04 07
30604 Hannover

Fax: 05 11/53 52-361
E-Mail: <user>@ix.de
Web: www.ix.de

Direktwahl zur Redaktion: 05 11/53 52-387

Für telefonische Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion wie gewohnt während der Lesersprechstunde zur Verfügung. Und zwar:

Montag bis Freitag, 11 bis 12 Uhr

Bitte nur während der genannten Zeiten anrufen und möglichst die angegebene Durchwahl benutzen.

<Durchwahl>	<user>	
-387	post	Redaktion allgemein
-377	avr	(André von Raison)
-590	ck	(Christian Kirsch)
-387	cle	(Carmen Lehmann)
-374	hb	(Henning Behme)
-379	jd	(Jürgen Diercks)
-386	js	(Jürgen Seeger)
-367	ka	(Kersten Auel)
-153	mm	(Michael Mentzel)
-787	mr	(Michael Riepe)
-373	rh	(Ralph Hülsenbusch)
-689	sun	(Susanne Nolte)
-368	un	(Bert Ungerer)
-535	ur	(Ute Roos)
-384	wm	(Wolfgang Möhle)

Listing-Service:
Sämtliche in iX seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich:
ftp.heise.de/pub/ix/

Da viele mir bekannte Systeme durchaus seit Jahren laufen, ohne jemals Probleme zu machen, halte ich es aus meiner Erfahrung für sinnvoller, die maximale Größe der Logfiles angemessen an die Größe der zur Verfügung stehenden Partition anzupassen. So vermeidet man ein Vollaufen der Partition und minimiert (je nach Platz) das Risiko, eine Fehlermeldung zu verlieren. Darüber hinaus besitzt diese Konfiguration den Vorteil, dass der/die so konfigurierte/n Server nicht ausgerechnet zu einem Zeitpunkt Probleme macht, in der man als Admin gerade mit einem fehlerhaften System beschäftigt ist, dass bei allen anderen Systemen für eine u.U. extrem erhöhte Anzahl von Logmeldungen führt.

HOLGER PATZELT

Sie haben natürlich recht damit, dass solch eine Konfiguration ausschießlich für einen kurzen Zeitraum (nämlich der Fehlersuche) sinnvoll ist. Es ist immer schwierig, eine breite Zielgruppe anzusprechen, da die Vorkenntnisse sehr unterschiedlich sind, daher hätte ich das konkret erwähnt sollen. (Karolin Seeger)

Verhalten über Oberfläche ändern

(Softwareentwicklung: Visual Studio 2008; *iX* 3/08; S. 56)

In Ihrem Bericht über das neue Visual Studio 2008 findet sich auf Seite 60 in der rechten Spalte folgende Aussage: „Eine unangenehme Eigenart des Designers ist, dass die Verweise in der Datenkontext-Klasse auf die Geschäftsobjektklassen deren Namen mit einem angehängten kleinem „s“ erhalten. […] Zwar kann man die LINQ-to-SQL-Entität im Designer umbenennen und damit auch die Klassennamen in den Singular setzen, aber dies ist mühsam. Und das „s“ für den Plural wird man gar nicht los.“

Zumindest in der auf meinem Rechner installierten Visual C# 2008 Express Edition kann man das von Ihnen beschriebene Verhalten sehr wohl über die Oberfläche ändern. Unter Tools -> Options … -> Knoten Database Tools -> O/R Designer findet sich die Option „Pluralization of names“, deren Property „Enabled“ auf den Wert False gesetzt das gewünschte Verhalten hervorbringt. Wichtig ist, dass in dem Dialog die Checkbox „Show all settings“ gesetzt ist.

Dieses Verhalten dürfte dem Kommandozeilenargument /pluralize des dem O/R-Designers angebundenen Tools Sqlmetal.exe entsprechen, welches die Entität-Klassen automatisch erzeugt.

KARSTEN KRUG, BONN

Shotcodes besser für mobile URLs

(World Wide Web: Der mobile Link ins Internet – 2D-Barcodes; *iX* 3/08; S. 116)

Ein bisschen merkwürdig fand ich, dass auf Shotcodes überhaupt nicht eingegangen wird (siehe www.shotcode.com). Der Ansatz scheint gerade für mobile URLs sehr interessant zu sein, da er weniger Information speichern kann, dafür aber auch eine bessere Erkennungsrate bei schlechter Barcode-Qualität aufweist (z.B. nach mehrmaligem Faxen oder beim Heranzoomen innerhalb eines Schaufensters). Außerdem kann man die Ziel-URLs später noch beim Betreiber ändern, ohne dass der Shotcode geändert werden muss.

MARTEN LEHMANN, POTSDAM

Semacode war einer der Ersten

(World Wide Web: Der mobile Link ins Internet – 2D-Barcodes; *iX* 3/08; S. 116)

Warum wurde der Pionier Semacode in dem Artikel „Alles klickt“ in der aktuellen Ausgabe nur mit einem Halbsatz erwähnt und bei der Linksammlung vollständig vergessen? Das finde ich ungerecht, da er einer der ersten war, die brauchbare Readers auf Handy-(S60)-Basis angeboten hat, und als Forscher bin ich sensitiv bezüglich Credit eingestellt … Ehre, wem Ehre gebührt!

DR. ALEXANDER K. SEEWALD (ÖSTERREICH)

Ergänzungen und Berichtigungen

(Vorschau: Produktlinien sparen Entwicklungskosten; *iX* 3/08, S. 186)

Aus redaktionellen Gründen musste leider der Artikel zur Produktlinienentwicklung in Ausgabe 5/08 verschoben werden.



Stimmen zur Cebit

Karl-Heinz Streibich, Vorstandsvorsitzender der Software AG: „Für uns die Cebit hervorragend gestartet, und wir hatten schon am ersten Tag deutlich mehr Kunden und Besucher als letztes Jahr. Es sind Fachbesucher, die mehr als früher die Cebit als Wettbewerbsshow nutzen.“

Bernd Völcker, Vorstand der Infopark AG: „Das neue Profil der Cebit ist deutlich zu spüren. Mit dem angepassten Messekonzept sind wir sehr zufrieden. Die Einbindung von Kongressen und Foren spricht das Fachpublikum optimal an.“

Stefan Backes, Director Marketing Central Europe Novell: „Wir unterstützen die Umstrukturierung der Messe. Die Ausrichtung auf das Business-Publikum kommt uns entgegen. Durch den Umzug in die Halle 2 und deren Fokussierung hatten wir einen besseren Zugang zu unserer Zielgruppe.“

Hannes Schwaderer, Geschäftsführer der Intel GmbH: „In der Zeit von Dienstag bis Freitag findet der IT-Profi die für ihn relevanten Informationen, das Wochenende steht den Privatnutzern zur Verfügung. Das reflektiert unser Konzept, das einen Umbau des Standes in der Nacht von Freitag auf Samstag beinhaltet.“

Stefan Engel, Geschäftsführer Acer Computer GmbH: „Überzeugend war in diesem Jahr in unseren Augen das neue Drei-Säulen-Messekonzept mit der klaren Gliederung Handel, öffentlicher Sektor und Wirtschaft.“

Volker Merk, Deutschland-Chef SAP: „Neu ist, dass die Cebit noch stärker an Themen und Lösungen orientiert ist – was eine perfekte Deckung mit den Bedürfnissen der Besucher bedeutet. Neu ist auch das umfangreichere und besser gebündelte Kongressprogramm.“

Achim Berg, Vorsitzender der Geschäftsführung Microsoft Deutschland GmbH: „Während der gesamten Messe hatten wir stets sehr gute Gespräche mit den Fachbesuchern. Diese waren gut vorbereitet, und in vielen Fällen ging es um konkrete Projekte.“

IT-Messe: Erfolgreich wie nie zuvor

Neues Konzept

Wolfgang Möhle

Als Ernst Raue die abschließende Pressekonferenz eröffnete, hörte man noch in den hinteren Reihen den Fels von seinen Schultern fallen. Die Cebit-Macher hatten viel riskiert – und alles gewonnen.

Wir haben Wort gehalten. Die neue Cebit hat ein scharfes Profil, eine klare Struktur und deutlich mehr Inhalt“, so der für die Cebit verantwortliche Ernst Raue. Die vier Ausstellungsbereiche – Business Solutions, Public Sector Solutions, Home und Mobile Solutions sowie Technology und Infrastructure – erlaubten auf der diesjährigen Cebit eine weitgehend nach Schwerpunkten gruppierte Hallenbelegung und dadurch auch eine räumliche Trennung von B2B und B2C.

Die direkten und kürzeren Wege sind ja nur ein Angebot: Die Messe als Plattform nutzen müssen Aussteller und Besucher. Und da kamen in diesem Jahr einige positive Punkte zusammen. Zum einen die immer noch ordentliche Gesamtkonjunktur einschließlich der Hoffnung, dass sich die Wirtschaftslage in absehbarer Zeit nicht grundlegend ändert. Zum anderen die Bereitschaft, in IT zu investieren, entweder als Ersatzbeschaffung, weil man schon einige Zyklen ausgelassen hat oder weil Expansionen und neue Geschäftsfelder angesagt sind. „Die Bereitschaft zu investieren war sehr groß“, so August-Wilhelm Scheer als Bitkom-Chef und Vertreter der Aussteller.

Mit dem Thema „Green IT“ traf man zudem den Zeitgeist. Niemand hat erwartet, dass es nach einer Woche für alle diesbezüglichen Probleme innerhalb der IT eine Lösung geben kann. Auch wenn viele Aussteller das Thema aufgegriffen haben, schien es doch oft marketinggetrieben, selten waren die Aussagen mit harten technischen Fakten belegt. Eine Sensibilisierung der Kunden ist aber erreicht und wenn es nur darum geht, die explodierenden Stromkosten zu senken. Jetzt schlägt die Stunde der Fachpresse, für die notwendige und unabhängige Aufklärung zu sorgen.

Traditionsgemäß erfüllt die Cebit die Rolle als riesige branchenspezifische Job- und Kontaktbörse. Unter dem Label „Job & Career Market“ bemühten sich IT-Firmen, das Interesse der Besucher an ihrem Unternehmen zu wecken. Besucher waren hier Studenten kurz nach oder vor dem Abschluss oder einfach nur Wechselwillige. Für diesen Markt stellte die Cebit sehr viel mehr Ausstellungsfläche als im letzten Jahr zur Verfügung.

Für die, die eine erfolgreiche Messe nur im Zahlenspiegel sehen können, hat Raue zum Schluss der Veranstaltung noch ein paar Zahlen nachgeschoben: knapp unter 500 000 Besucher, davon mehr als 100 000 aus dem Ausland, fast 80 % haben sich als Fachbesucher geoutet, und die mehr als 5800 Aussteller kamen aus 77 Ländern. Für Scheer ist die Besucherzahl ohnehin kein Maßstab: „Nicht die absolute Zahl ist wichtig, sondern dass die richtigen, sprich die potenziellen Kunden kommen.“ Und das war in diesem Jahr augenscheinlich der Fall.

Nach der Cebit ist vor der Cebit: 2009 beginnt sie am Dienstag, den 3. März, und dauert bis Sonntag, den 8. März. (WM)





Prolog: Steve Ballmer sprach auf der Eröffnungsfeier am Vorabend der Cebit von der vierten IT-Revolution, dem realen Web 2.0 und träumte von der fünften, der nun wirklich papierlosen Kommunikation. Weniger visionär als Microsofts CEO warb der Präsident des diesjährigen Cebit-Partnerlands Frankreich, Nicolas Sarkozy, für eine engere Zusammenarbeit zwischen seinem Land und Deutschland, die in konkrete Projekte wie beispielsweise der Entwicklung neuer Hochleistungsrechner münden sollte.





Epilog: Eine überaus positive Bilanz der Cebit 2008 zog Ernst Raue, Mitglied des Vorstandes der Messe AG und für die Cebit verantwortlich, mit seinem unzweideutigen Resümee: „Wir erlebten die beste Cebit aller Zeiten.“ Da mochte auch der Chef des IT-Lobbyverbandes Bitkom, August-Wilhelm Scheer, nicht zurückstehen und unterstrich, durch eigene Erfahrungen angereichert, seine ebenfalls ausgesprochen positive Sichtweise der sechs Messetage.



Speicher im Hallendickicht der Cebit

Nicht wenige der großen Namen der Speicherbranche fehlten dieses Jahr in Hannover, der Rest war verstreut über das Gelände oder irgendwo als Unteraussteller versteckt. Wer nicht bis zum Branchentreff SNW Europe im Herbst warten wollte, konnte dennoch einiges entdecken.

Sandisk etwa präsentierte einen Flashback-Adapter genannten Einschub für den Expresscard-Slot, der in den neueren Notebooks den PCMCIA-Standard ablöst. Eine OEM-Software speichert zusätzlich alle neuen Dokumente oder Ordner kontinuierlich auf einer Flashcard, die im Adapter Platz findet – eine mobile Anwendung von Continuous Data Protection (CDP), die wahlweise, etwa für Vielreisende, sogar automatisch die Daten auf dem Stick verschlüsselt. Adapter und Backup-Software kosten 30 Euro, eine 32 GByte fassende Flashcard derzeit noch etwa 500 Euro. IBM Tivoli hatte auf der Softwareseite vor etwa zwei Jahren mit Continuous Data Protection for Files ein ähnliches Angebot herausgebracht (Preis: etwa 50 Euro). Mit „Vaulter“ plant Sandisk zudem, eine Kombination aus SSD (Solid State Disk) und Festplatte für Notebooks herauszubringen: Auf der SSD sollen Betriebssystem und Applikationen untergebracht werden, was das Hochfahren und Ausschalten beschleunigt, während die Disk für schnelle Lese- und Schreibzugriffe von Dateien zur Verfügung steht.

Bei IBM standen Lösungen für File Area Networks (FAN) im Vordergrund. Auf der Hardwareseite setzt IBM Bladecenter als Basis-Appliances ein, während als Middleware das im High Performance Computing verwendete General Parallel File System (GPFS) zum Einsatz kommt. GPFS hat viele ILM-Funktionen für Speicherklassen bekommen, Flash Copy und Tape-Anbindung sind ebenfalls integriert. Für die Datenmigration sorgt der Tivoli Storage Manager (TSM). Darüber befinden sich die Skill Out File Services (SOFS), die Policy-basiert alle Dateisysteme aus der Open-Systems-Welt integrieren können.

Sun stellte auf der Cebit gleich mehrere Neuerungen im Storage-Bereich vor. Neben dem Bandlaufwerk T9840D, das Sun als „neues Fast Access Enterprise Tape Drive“ bezeichnet, ist das vor allem die SL3000, die mit der gleichen Technik wie das Enterprise-Modell SL8500 daherkommt: Sie verfügt ebenfalls über Redundanz bei den Robots (Tallbot, Handbot) und bei den Power- und Cooling-Funktionen. Zudem kann sie durch physische und logische Partitionierung Mainframe- und Opens-Systems-Daten in einem Gerät speichern. Außerdem bietet der Hersteller nun Capacity on demand an.

Hitachi Data Systems (HDS) bietet derweil NAS-Systeme von Bluearc an, die unter anderem mit der Replikationstechnik (Truecopy) von HDS ausgerüstet sind. Als weitere Neuerung offerierte der Hersteller, der seine Kunden vor allem bei Highend-Arrays hat, die VTL-Modelle 500M, 1000L und 1000E, die über integrierte Deduplizierungsfunktionen von Diligent verfügen. Außerdem präsentierte das japanische Unternehmen mit der Data Discovery Suite eine Index- und Search-Technik, die NAS- und Archivierungsumgebungen zusammen durchforsten kann.

Auch Falconstor glänzte mit Deduplizierung, die Bestandteil der neuen VTL Enterprise Edition 5 ist. Nachdem jetzt kein Storage-Anbieter mehr ohne diese Technik am Markt auftritt, fragt man sich unwillkürlich, ob die Branche bisher die Tatsache verschlafen hatte, dass in Unternehmen unzählige Datenduplikate existieren. Am Datenwachstum allein kann es nicht liegen – das explodiert ja schon seit Jahren. Anwender sollten behutsam auf den neuen Zug aufspringen, denn unüberlegt installierte Datei-Entrümpelung kann schnell auf Kosten der Performance beim Datenspeichern gehen – schließlich gilt es die Duplikate erst einmal zu finden.

Martin Jetter, der Deutschland-Chef von IBM, formulierte dieses Jahr den Satz: „Die Halle 2 ist die neue Halle 1.“ Bleibt zu hoffen, dass die Messe AG nächstes Jahr endlich eine dezidierte Speicher-Halle, mit welcher Nummer auch immer, präsentieren kann. Das würde den Komfort für die an Storage interessierten Besucher ungemein erhöhen, die sich nicht mehr im Dickicht der Hallen verlieren müssten. *Hartmut Wiehr*

Schlafende Festplatten

Als Alternative zu Band- und optischen Archiven ist seit einiger Zeit das Massive Array of Idle Disks (MAID) im Gespräch. Es benötigt bei gleicher Kapazität erheblich weniger Energie als die immer bereiten klassischen RAID-Systeme, deklassiert optische Jukeboxen in puncto Datendurchsatz und erlaubt im Gegensatz zu Bandarchiven schnelle Zugriffe auf einzelne Dateien. Allerdings haben nur wenige Anbieter ein MAID-System im Portfolio.

Zu den MAID-Pionieren gehört Copan Systems (www.copansystems.com). Auf der Cebit stellte die Firma ihr Enterprise MAID aus. Das System setzt sich aus ein bis acht „Shelves“ mit jeweils acht Platteneinschüben zusammen. Jeder Einschub enthält 14 SATA-Festplatten – setzt man Terabyte-Platten ein, beträgt die Bruttokapazität maximal 896 TByte. Davon ist allerdings höchstens ein Viertel im Zugriff, den übrigen Platten schaltet das System den Strom ab. Dabei verwendet es ein ähnliches Nutzungsmuster wie ein Desktop-Rechner, was der Lebensdauer der SATA-Laufwerke zugutekommt.

Logisch teilt das Enterprise MAID die 112 in einem Shelf vorhandenen Platten in Vierergruppen ein. Eine dient als Spare Pool, die übrigen bilden jeweils ein RAID 5. Um Hot Spots zu vermeiden, liegen die Platten einer RAID-Gruppe über das gesamte Shelf verstreut. Aus demselben Grund verteilen sich die gerade aktiven RAIDs auf alle Shelves im Rack. Längere Zeit nicht genutzte Platten weckt das System spätestens nach 30 Tagen für eine Runde „Disk-Aerobic“ auf. Zeigt sich dabei, dass ein Laufwerk auszufallen droht, kopiert es seine Daten vorsorglich auf eine Spare-Platte, bevor es zum Ausfall und dem damit verbundenen aufwendigen Rebuild des RAIDs kommt.

Neue Mainframe-Generation

Unter dem Namen z6 hatte IBMs neue Mainframe-Serie bereits im Vorfeld die Gerüchteküche angeheizt; auf der Cebit war nun der neue Mainframe System z10 zu bewundern. Den Codenamen z6 trug der zugehörige Prozessor im eClipz-Projekt, in dem IBM an der Zusammenführung seiner Architekturen arbeitet. Er sollte die Nähe zum Power6 kennzeichnen: Beide CPUs werden im 65-nm-Prozess gefertigt und weisen Gemeinsamkeiten im Grundlayout auf.

Im Vergleich zum Vorgänger z9 will Big Blue bis zu 100 Prozent mehr Rechenleistung aus dem neuen System z10 Mainframe herausholen. Verantwortlich dafür sind 64 z10-EC-Prozessoren mit je vier Cores und 4,4 GHz Taktfrequenz – in einem System z9 EC sind es maximal 54 z9-CPUs mit nur 1,7 GHz. Als Betriebssystem dient auf der z10 z/OS V1.9. Die Version 1.10 soll im Herbst folgen. Außerdem stehen Linux für System z, der Hypervisor z/VM und z/TPF zur Verfügung.



Aufgeschnitten und in Glas gelegt: Auf dem IBM-Stand hatten die Cebit-Besucher die Gelegenheit, dem z10-Mainframe im 24"-Rack mit integrierter Wasserkühlung in die Eingeweide zu schauen.

Neue Kühlkonzepte auf der Cebit

Warme Winde

Susanne Nolte

Während die Hersteller von IT-Systemen und -Komponenten ihren Kunden das „grüne“ Gewissen erst einimpfen wollen, sehen sich Rechenzentren mit einer anderen Herausforderung konfrontiert: Schleunigst müssen Alternativen zur bisher recht energieintensiven Kühlung her.

Da gerade die Rechenzentren mit dem steigenden Stromverbrauch zu kämpfen haben, kam auf der Cebit kein Rechenzentrumsausstatter um die Themen Energieeffizienz und Stromsparen herum. Dadurch war wohl auch die plötzliche Inflation von Kaltgang- respektive Warmgangeinhausungen in Halle 12 zu erklären.



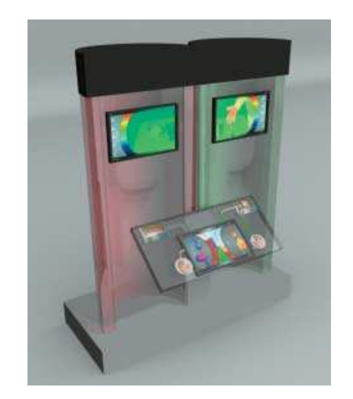
Ein Gang zwischen zwei Rack-Reihen mit Doppelboden, Glasdach und Schiebetüren versehen sowie ein geschlossener Luftkreislauf bilden den Kaltgang von Schäfer IT-Systems (Abb. 1).

Den abgeschlossenen Warmgang hatte sich APC schon vor einiger Zeit patentieren lassen: Zwei Reihen Racks drehen dem mit Glasdach und Schiebetüren vom Rest des Rechenzentrums getrennten Gang den Rücken zu. Die Lüfter der darin befindlichen Systeme ziehen die Luft aus der temperierten Umgebung und blasen sie in den abgedichteten Gang, wo sie den Luft/Wasser-Wärmetauschern nicht entkommen kann. Konzipiert ist das System vor allem für die Hotspots, verursacht durch Blades oder 1-U-Server.

Auf den Ständen der Mitbewerber waren die Gegenstücke zu bewundern: Kaltgänge sind in der Breite grundsätzlich großzügiger ausgelegt, da sie ausreichend Platz für die Montage der Server bieten müssen: Rechts und links von Kaltgängen stehen sich die Server-Racks frontal gegenüber. Schäfer IT-Systems etwa arbeitet mit Doppelbodenplatten zwischen und unter den Racks, aus denen kalte Luft zu den Servern strömt. Die geschlossenen Rückseiten der SP-20-Racks führen die warme Luft wieder zum Wärmetauscher zurück. Die 60 × 60 cm^2 großen Doppelbodenplatten namens Swap Panel 9 bestehen aus neun Quadraten, die sich nach Bedarf mit geschlossenen, gelochten oder Kabelführungseinsätzen versehen lassen.

Da solche Systeme eher für Wärmeproduzenten der mittleren Gewichtsklasse geeignet sind, hatte Schäfer daneben sein geschlossenes, wassergekühltes Uniqle-Rack für thermische Schwergewichte aufgebaut.

Mit der Kühlung zukünftiger Rechenzentren beschäftigen sich die Forscher des Zurich Research Laboratory in Rüschlikon. Ihr Ziel: Die von den IT-Systemen erzeugte Wärme wollen sie für Heizanlagen zurückgewinnen. Voraussetzung dafür ist eine wesentlich höhere Wassertemperatur, als sie bisher in Rechenzentren vorkommt: Da für Luft/Wasser-Wärmetauscher der Wasservorlauf (Warmwasser) kälter sein muss als der Luftrücklauf (kalte Luft), erreicht das durch die Systeme erhitzte Wasser bei den bisher üblichen Klimaanlagen keine 30 °C.



Auf dem IBM-Stand hatten die Schweizer Forscher das vereinfachte Modell ihres „Zero Emission Data Center“ aufgebaut – hier als gerendertes 3D-Modell (Abb. 2).

Die Schweizer Forscher schlagen deshalb einen anderen Weg ein: Statt mit gekühlter Luft wollen sie die Systeme direkt mit warmem Wasser kühlen. Momentan existiert ein Prototyp einer direkten Wasserkühlung für CPUs, dessen verkleinertes Modell auf der Cebit aufgebaut war: Die heißlaufenden Recheneinheiten erwärmen das 45 °C warme Kühlwasser auf 50 °C und höher; das lässt sich dann ohne den Einsatz zusätzlicher und vor allem energieverschlingender Wärmepumpen zum Heizen verwenden.

Momentan arbeiten die Wissenschaftler an der Anpassung des Kühlsystems an andere Komponenten und Systeme, etwa an ganze Serverinnenräume und Disk-Subsysteme, deren Laufwerke nicht für solch hohe Temperaturen ausgelegt sind.

Bitkom-Leitfaden zur Energieeffizienz im Rechenzentrum

Mit praktischen Hinweisen will der Bitkom Hersteller und Betreiber bei Planung, Bau und Betrieb von Rechenzentren unterstützen. Die hat der ITK-Branchenverband in einem Leitfaden „Energieeffizienz im Rechenzentrum“ zusammengefasst, den er als Vorabversion auf der Cebit verteilte. Denn nach seiner Ansicht besteht eine solide Unkenntnis vor allem über die Energiekosten, da Unternehmen diese häufig als Gemeinkosten abrechnen.

Allein durch das Messen des Energieverbrauchs lassen sich unnötige Stromfresser ausmachen. Neue Messmethoden und eine Visualisierung etwa der Temperaturverteilung im Rechenzentrum versprechen noch genauere Erkenntnisse.

Eine Analyse zeigt: Nur die Hälfte des Energieverbrauchs entsteht direkt durch die IT – die andere Hälfte verbrauchen Klimatisierung und unterbrechungsfreie Stromversorgung (USV). Diesen beiden Themen sind zwei große Kapitel gewidmet.

Gerade beim Thema USV gilt es, die Wechselwirkung von Effizienz und Sicherheit zu berücksichtigen. Entscheidend ist der Wirkungsgrad der USV. Allein durch die Verlustleistung verschiedener USV-Typen entstehen im schlimmsten Fall pro Jahr Mehrkosten von über 10 000 Euro und ein CO_2-Ausstoß, der 300 000 gefahrenen Kilometern eines PKW entspricht. Über eine Zielvorgabe für den Wirkungsgrad von USVs haben sich EU und Hersteller nach Angaben von Bitkom kürzlich geeinigt.

Zwei relativ kurze Kapitel beschäftigen sich mit der Optimierung von Hard- und Software, etwa durch Virtualisierung, sowie dem Energy Contracting, das das Management von Kühlung und Strom vereinfachen soll.

Für die Datenspeicherung empfehlen die Autoren unter anderem, wie dem Löschen nicht benötigter Dateien, ein Information Lifecycle Management (ILM), das den am besten geeigneten Speicherplatz bestimmt: Nur Daten, die schnell verfügbar sein müssen, bleiben auf teuren Speichern mit hohem Energieverbrauch – andere rutschen auf Nearline- oder Offline-Storage. Archivierte Daten gehören auf Offline-Medien.

Barbara Lange



Cebit im Energiespar-Hype

Grüner Schaum

Hartmut Wiehr

Green IT hat einen rationalen Kern – Energieverschwendung in Rechenzentren, im Büro oder zu Hause. Auf der anderen Seite vergaloppieren sich manche Marketingstrategen bei dem Bemühen, ihr Unternehmen als das allergrünste herauszustellen.

Manche lassen jedes Mal einen Baum pflanzen, sobald ein Computer das Werksgelände verlässt. Andere spenden fleißig an Umweltinitiativen oder – noch besser – gründen gleich selbst eine. AMD war in vorderster Linie beim Green Grid dabei, Intel hat die Climate Savers Computing Initiative aus der Taufe gehoben. Wer sich auf der Cebit ins Green IT-Village in Halle 9 vorwagte, konnte dort zum Beispiel auf freundliche Vertreter der Klimaretter treffen – mit Intel-Namensschild am Revers.

Sie haben sich das ehrgeizige Ziel gesetzt, die bestehenden etwa eine Milliarde zählenden IT-Geräte auf der Welt bis zum Jahr 2010 durch 50 % energieeffizientere ersetzen. Erreichen wollen sie das durch eine Aufklärungskampagne, die sich an Privatanwender richtet, zum Beispiel mit Energiespartipps: „1. Turn on – and leave on – computer power management. 2. Buy energy-efficient PCs and servers. 3. Spread the word“. Zusätzlich wollen die 175 Mitgliedsfirmen bei sich selbst anfangen und Stromsparpläne umsetzen. Die Verlängerung der Hardware-Lebenszeit und das Einsparen beispielsweise von gut 1,5 MWh pro neu produziertem PC gehören sicherlich nicht dazu, das würde nur die Gewinne schmälern.

Letztlich sind es wir alle, die sich an der Umwelt versündigen. Doch die Suche nach den Verursachern geht weiter – und momentan ist die IT an der Reihe. Die Hersteller halten es für ein Verkaufsargument, auf ihre eigenen guten Taten zu verweisen. Beispiel Nummer eins: „Overland Storage hat immer Wert darauf gelegt, energieeffiziente Produkte zu entwickeln – ohne dies ‚Green IT’ zu nennen.“ Sprich: Der Hersteller war schon immer „grün“, es fiel nur niemandem auf. Zweites Beispiel: Fujitsu Siemens Computers fing schon 1988 – damals hieß man noch Siemens-Nixdorf – mit dem Recycling von IT-Produkten an. Wer damals schon so grün war, ist es heute erst recht. Und kann – nachdem mechanische Ausschalter in Vergessenheit geraten sind – gleich den „ersten Null-Watt-Monitor“ präsentieren, sowie eine Umfrage, die schon wieder ergibt, dass die Menschen für Umwelt und Green IT sind und sogar mehr Geld dafür ausgeben würden – was die Marketing-Strategen besonders freuen dürfte. Beispiel Nummer drei: Hitachi Data Systems (HDS) ist schon seit Anfang der 70er-Jahre des letzten Jahrhunderts irgendwie „grün“, wie Firmenvertreter stolz auf einer Pressekonferenz verkündeten – damals baute man umweltfreundliche Gebäude. Außerdem verkaufe die Muttergesellschaft Hitachi heute umweltfreundliche Eisenbahnen. So viel geballte Kompetenz muss vermutlich zwangsläufig auf die IT-Sparte abfärben.

Unternehmen, die noch älter sind, werden sicherlich bald mit weiteren Überraschungen aufwarten. Was Anbieter übersehen, die heute mit Green IT hausieren gehen, ist die Tatsache, dass Umweltthemen spätestens mit den Grünen in Deutschland und Al Gore in den USA moralisch hoch besetzt sind: Jeder nickt mit dem Kopf, wenn man ihn auf das Thema anspricht, oder spendet sogar ein paar Euro nach einer Flugreise. Doch ob man sich deswegen gleich ein Notebook mit Bambusüberzug zulegt, steht auf einem anderen Blatt. Viel Vergnügen also bei dem Kampf um die Geldbeutel einer betuchten Klientel. Firmen haben ihre eigenen Gründe, warum sie sich für ein bestimmtes Produkt entscheiden. Da braucht es vielleicht doch bessere Argumente. (mr)

Greenpeace auf der Suche nach grüner Elektronik

In seiner Studie „Searching for Green Electronics“ vergleicht Greenpeace 37 Produkte von 14 Herstellern anhand von Kriterien wie Energieeffizienz und Wiederverwertbarkeit sowie der verwendeten Chemikalien (www.greenpeace.org/international/press/reports/searching-for-green-electronics). Ergebnis: Trotz guter Ansätze bleibt viel Raum für Verbesserungen. Viele Hersteller reduzieren zwar Giftstoffe, verbessern Energieeffizienz, Lebenszyklus und Recycling. Ein wirklich grünes Produkt und einen umfassenden umweltfreundlichen Ansatz, der den gesamten Lebenszyklus berücksichtigt, gebe es aber noch nicht, betonen die Umweltschützer.

Endkunden sollten sich nicht fragen müssen, ob sie ein giftfreies oder ein energieeffizientes Gerät kaufen wollen. Als Schlüssel für ein umfassend grünes Produkt sieht Greenpeace die Kombination aller positiven Ansätze in einem Gerät.

Nur 14 Unternehmen haben auf die Anfrage von Greenpeace reagiert und ihre drei „grünsten“ Produkte zum Testen eingereicht. Die besten Ergebnisse erzielten der Laptop Sony Vaio TZ11, das Mobiltelefon Sony Ericsson T650i und der PDA P1i von Sony Ericsson. Aber selbst diese drei erfüllen nur die Hälfte der Kriterien. Nicht teilgenommen haben Acer, Apple, Asus, Creative, Microsoft, Nintendo, Palm und Sharp.

Barbara Lange

E-Energy-Preis

Sechs Gewinner des Wettbewerbs „E-Energy: ITK-basiertes Energiesystem der Zukunft“ (www.e-energie.info) gab Dagmar Wöhrl, parlamentarische Staatssekretärin beim Bundeswirtschaftsministerium (BMWi) bekannt. Vier der ausgewählten Forschungsvorhaben will das BMWi mit 40 Mio. € fördern, die anderen zwei wird das Bundesumweltministerium mit 20 Mio. € unterstützen.

„Die weitere Liberalisierung des Energiemarktes wird ohne ITK nicht gelingen“, so Wöhrl. Hierfür sei eine breite Zusammenarbeit von ITK- und Energiebranche notwendig. Ziel des Projektes E-Energy, seit 2006 Leuchtturmprojekt der Bundesregierung, ist es, die Informationstechnik durchgängig für die Optimierung der Elektrizitätsversorgung nutzbar zu machen. ITK soll die Versorgungssicherheit, Wirtschaftlichkeit und Umweltverträglichkeit sicherstellen und etwa die Mischung von zentraler und dezentraler Energieerzeugung koordinieren.

Als Geräte wie die Waschmaschine oder der Mikrowellenherd vor ein paar Jahren internetfähig wurden, haben Viele gelacht . Doch in Zukunft sollen Haushaltsgeräte ihren Einsatz selbstständig koordinieren und erst dann anspringen, wenn der Strom besonders günstig ist.

Das will man in sechs Modellregionen entwickeln. Das Projekt eTelligence (www.etelligence.de) etwa will die in der Region Cuxhaven zu einem hohen Anteil erzeugte Windenergie in die Netze integrieren. Ein zentrales Portal soll Erzeuger, Verbraucher, Dienstleister und Netzbetreiber zusammenführen. Haushalte können online ihren Stromverbrauch ablesen und anpassen. Großverbraucher wie Kühlhäuser sollen die Möglichkeit bekommen, durch eine Senkung der Kühltemperatur die bei gutem Wind ausreichend vorhandene Energie zu „speichern“ und bei Flaute die Stromaufnahme zu drosseln.

Weitere Fördermittel gehen an die Modellstadt Mannheim, E-DeMa (Rhein-Ruhr-Gebiet), RedModHarz (Harz), Meregio (Karlsruhe/Stuttgart) und Smart W@tts (Aachen).

Barbara Lange



Energielabel für Computer

Grüner Engel

Michael Riepe

„Wenn Du nicht mehr weiter weißt, bilde einen Arbeitskreis.“ Gemäß dieser Devise sollen jetzt Kommissionen und Zertifikate die IT aus dem Energiesünderpfuhl ziehen.

Für unzureichend hält die Linkspartei die bisherigen Bemühungen der Computerindustrie zur Senkung des Energieverbrauchs. Abhilfe soll eine Kennzeichnungspflicht schaffen. Das geht aus einem Antrag hervor, den die Fraktion der Linken (die-linke.de) am 5. März eingereicht hat (www.bundestag.de/aktuell/hib/2008/2008_071/02.html).

Das vorgeschlagene Energielabel soll den Energiebedarf in verschiedenen Betriebszuständen – etwa Leerlauf und Volllast – sowie im Standby- und Soft-off-Modus bereits vor dem Kauf sichtbar machen. Ausgeschaltete Geräte sollen nach dem Willen der Antragsteller überhaupt keinen Strom mehr aufnehmen, für den Verbrauch im Leerlauf oder Standby-Modus soll es „ambitionierte“ Höchstgrenzen geben.

Eine dafür einzurichtende Kommission aus Umwelt- und Verbraucherschützern, Herstellern, Wissenschaftlern und Vertretern der zuständigen Behörden soll alle drei Jahre die Richtwerte überprüfen und gegebenenfalls neu festlegen. Nach dem sogenannten „Top-Runner-Prinzip“ bestimmen dabei die Besten die Höhe der Hürden, die alle anderen innerhalb eines bestimmten Zeitraums zu nehmen haben.

Außerdem sollen die Geräte ähnlich wie Kühlschränke in Effizienzklassen eingeteilt werden – wobei der Antrag die nicht unwichtige Frage offenlässt, wie die Leistung des Geräts und damit seine Energieeffizienz zu bestimmen ist. Der TÜV Saarland (www.tuev-saar.net) etwa, dessen Tochter Tekit (www.tekit.de) ein vergleichbares Label für Archivsysteme entwickelt und auf der Cebit an zwei optische Jukeboxen von DISC und JVC vergeben hat, verwendet als Maß das Verhältnis zwischen Energiebedarf und Kapazität. Es wären jedoch auch andere Kriterien zu berücksichtigen, etwa der erreichbare Durchsatz oder die Zugriffszeit.

Auch konzentriert sich der Vorschlag der Linken auf den Endverbraucher-Markt – PCs, Notebooks und Peripheriegeräte. Er ignoriert die Belange etwa von IT-Abteilungen und Rechenzentren ebenso wie das dort vorhandene Sparpotenzial. Ihrer wollen sich IBM Deutschland und der TÜV Rheinland (www.tuv.com/de/) annehmen. Ziel der auf der Cebit besiegelten Kooperation ist die Entwicklung eines Standards für die Umweltverträglichkeit von Rechenzentren sowie – man ahnt es bereits – eines einschlägigen Zertifikats. Zur Kriterienbildung werde man international vorhandene Standards ebenso heranziehen wie praxisnahe und relevante Bewertungen der Energieeffizienz.

Insgesamt entsteht der Eindruck, dass das Angebot an freiwilligen Zertifizierungen in erster Linie den Zertifizierungsstellen dient – etwa den miteinander konkurrierenden regionalen Ausprägungen des Technischen Überwachungsvereins, die die Entwicklung solcher Zertifikate als Dienstleistung anbieten. Angesichts des Kreises der Auftraggeber und der produktbezogenen Auswahl der Prüfkriterien kann von „neutral geprüfter Qualität“ wohl kaum die Rede sein. Ohne einheitliche Standards sind die „Bapperl“ nicht mehr als ein Werbegag. Zumindest das spräche für eine gesetzliche Zwangsprüfung, etwa vergleichbar mit der Abgasuntersuchung bei Kraftfahrzeugen. (sun)



Anrufe und E-Mails unter einem Dach

Voxtron hatte die neue Version seiner Contact Center Suite Agentel 6.1 mitgebracht, eine Software, die E-Mails und Telefonate unter einer Oberfläche bündelt und regelbasiert an den fachlich oder zeitlich am besten geeigneten Mitarbeiter weiterleitet.

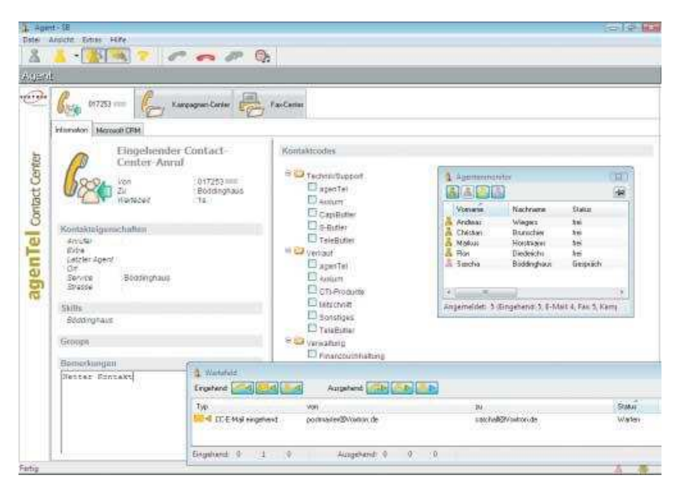
Durch eine Anbindung an vorhandene Unternehmens-Applikationen bekommt der Mitarbeiter Zusatzinformationen über den Anrufer auf seinem Bildschirm präsentiert, wodurch fundierte Gespräche möglich werden sollen. Eingehende Faxe leitet die Software als E-Mail an die jeweiligen Mitarbeiter weiter.

Als wichtiges Merkmal des Produkts hebt Voxtron die Unabhängigkeit vom Typ der vorhandenen Telefonanlagen hervor. Auch nach einem Wechsel der Anlage könne man das System weiter nutzen. Die Anbindung an die TK-Anlage erfolgt über Sprachkanäle (ISDN, analog, VoIP).

Mit dem OfficeClient erhalten die Mitarbeiter im Contact Center und im übrigen Unternehmen die gleiche Benutzeroberfläche, um dem Ziel der Verbindung von Front- und Backoffice näher zu kommen. Damit können auch die Mitarbeiter im Backoffice Funktionen wie das Präsenzmanagement nutzen. Außerdem ist es möglich, direkt aus Outlook und anderen Tapi-fähigen Programmen zu wählen.

Zu den Kunden von Voxtron gehören mittelständische und große Unternehmen, Banken, Versicherungen, Behörden, Handel und Industrie, Netzbetreiber und Hersteller von TK-Anlagen.

Barbara Lange



Unter einer Rufnummer erreichbar

Bei Cytel Technology AG war deren softwarebasierte VoIP-Telefonanlage CYTEL.iBX für Microsoft Windows zu sehen, die ISDN, analog, SIP und GSM mit Unified-Communications-Funktionen versieht. Nachrichten wie Fax, SMS, Telefon, Voice-Mail und SMS erscheinen unter einer einheitlichen Oberfläche, E-Mail nicht. Jeder Benutzer kann seine diversen Telefonnummern in bis zu vier Profile einbinden und ist damit immer unter einer Rufnummer erreichbar. Das Unternehmen richtet sich mit CYTEK.iBX an mittelständische Unternehmen mit fünf bis 300 Benutzern.

C4B: Anrufe im Webbrowser

C4B zeigte Version 2 des Produktes „XPhone CTI Mobility“, das eingehende Anrufe und Präsenzzustände in Echtzeit im Webbrowser signalisiert. Die Darstellung ist für Smartphones optimiert. Der Anwender kann die Anrufe per Mausklick annehmen. Zielgruppe sind Unternehmen mit mobil arbeitenden Mitarbeitern im Außendienst oder in Home-Offices.

Studie: VoIP und Unified Communications

Parallel zur Cebit stellen die Analysten von Berlecon Research ihre Studie „VoIP und Unified Communications 2008“ vor, die sich an ITK-Anbieter und -Dienstleister richtet. Demnach besteht ein großer Bedarf an Unified-Communications-Funktionen. Die Mehrheit von 150 im Januar und Februar 2008 befragten ITK-Entscheidern in deutschen Unternehmen mit mindestens 100 Mitarbeitern hält die Integration verschiedener Kommunikationskanäle und deren Einbindung in Office-Anwendungen für sehr wichtig. Vor allem versprechen sie sich eine bessere Unterstützung mobiler Mitarbeiter durch eine automatische Weiterleitung zum derzeit genutzten Endgerät über Find-Me-Follow-Me- und One-Number-Funktionen.

Die Analysten von Berlecon sehen VoIP als Voraussetzung für Unified Communications an, da unter technischen und wirtschaftlichen Gesichtspunkten nur dann eine Integration sinnvoll sei.

Mehr als die Hälfte der Unternehmen nutzt aber gar keine VoIP-Techniken. Nur 38 Prozent der Befragten verfügen über gemeinsame IP-Netze für Daten und Sprache, 25 Prozent nutzen eine IP-PBX.

Als Hindernis gilt die leidige Sicherheit. Die von Cisco Systems und T-Systems finanziell unterstützte Studie nennt eine Integration von Sicherheitsfunktionen daher als wichtigstes Entscheidungskriterium bei der Auswahl einer VoIP- beziehungsweise UC-Lösung. Auf Platz zwei steht die Administrierbarkeit mit 41 Prozent. 42 Prozent der Befragten können sich Managed Services als Betreibermodell vorstellen.

Barbara Lange

Siemens: Unified-Communications mit Videokonferenzen per Mausklick

„Open-Communication for the open minded“. Unter diesem Slogan stellte Siemens Enterprise Communications seinen neuen „Openscape Unified Communications Server“ vor. Nach eigenen Angaben ist dies die erste Softwareplattform auf dem Markt, die Video, Sprache, E-Mail, Instant Messaging, Festnetz, mobile Telefonie, Präsenzmanagement und Collaboration-Funktionen innerhalb einer UC-Lösung integriert.

Einsetzen lässt sich das Produkt in jeder IT- oder Telefonie-Umgebung. Es baut auf dem Session Initiation Protocol (SIP) und der serviceorientierten Architektur OpenSOA von Siemens auf und nutzt Hipath-8000. Eine Verbindung mit IBM Sametime oder Microsofts Office Communication Server ist möglich.

OpenScape Video, die dazugehörige Unified-Videoconferencing-Anwendung, soll standalone oder als Bestandteil des Openscale UC-Servers verfügbar sein. Als großen Vorteil hebt Siemens hervor, dass alle Mitarbeiter per Mausklick Videokonferenzen aufbauen können. Im Rahmen der Grüne-IT-Welle muss natürlich gesagt werden, dass dieses sowohl Reisekosten als auch CO_2-Ausstoß senkt. Bis zu sechs Standorte lassen sich zusammenschalten.

Der Openscape Unified Communications Server soll Ende April 2008 in drei Versionen auf den Markt kommen: Als Single-Server-Variante für bis zu 1000 Nutzer (Medium Edition), als Multiserver-Konfiguration für bis zu 100 000 Anwender (Large Edition) und als Hosted Edition, mit denen der Hersteller die speziellen Anforderungen von Service-Providern und Hosting-Unternehmen adressiert.

Barbara Lange

Anti-Spam-Dienstleister im Aufwind

Anbieter von Appliances und Dienstleistungen gegen Spam waren sich auf der Cebit einig darüber, dass es im vergangenen Jahr wieder einen Rekord an unerwünschten E-Mails gab. Die Zahl der Spam-Mails ist 2007 um ein Mehrfaches gestiegen, deren Größe jedoch etwa im gleichen Maße gesunken. Während die Spammer Anfang vergangenen Jahres mit Bilder-, PDF- und sogar MP3-Spam experimentierten, haben sie sich derzeit auf sehr kleine Mails verlegt.

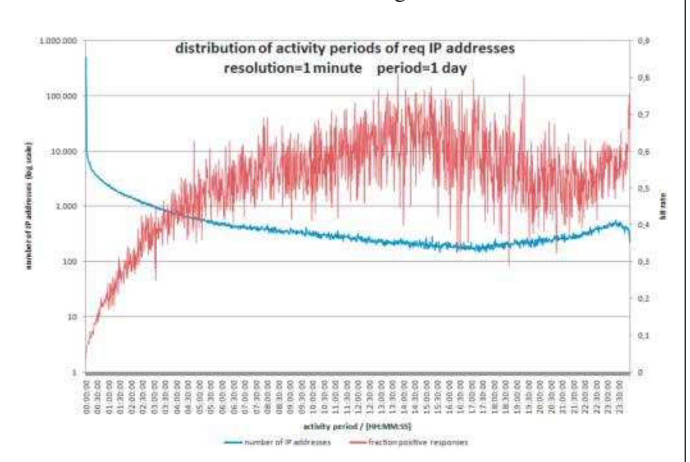
Mit Antispameurope und Eleven waren in Deutschland ansässige Dienstleister vertreten, die den kompletten Mail-Verkehr per MX-Eintrag auf sich umleiten. Sie sehen sich gegenüber den Geräteherstellern im Vorteil, da es angesichts der Tücken beim Betreiben eigener Mailserver einen Trend gebe, das Annehmen und Filtern von Mails komplett auszulagern.

In der Tat scheint den Appliance-Anbietern die reine Spam-Filterei nicht mehr zu genügen. Die Cisco-Tochter Ironport etwa führte ein „unternehmensweites Sicherheitsmanagement“ vor, das auch Data Leakage Prevention und Websicherheit umfasst. Reddoxx (vormals SfbIT) hat seinen Spamfinder mittlerweile um Produkte fürs Archivieren (Maildepot) und Verschlüsseln respektive Signieren (Mailsealer) ergänzt.

Spam kommt oft von „Einmal-IP-Adressen“

Zu den von Mailserver-Betreibern häufig eingesetzten Spam-Gegenmaßnahmen gehört das Abfragen von Blacklists, die IP-Adressen aufführen, von denen wahrscheinlich nur Spam zu erwarten ist. Während einer 24-stündigen Stichprobe Mitte Februar hat das Gelsenkirchener Institut für Internet-Sicherheit rund 17 Millionen solcher Anfragen an einen DNS-Slave-Server der von der *iX*-Redaktion betriebenen Blacklist gezählt (www.nixspam.org). Die Auswertung des Zahlengebirges ergab, dass gut ein Drittel der insgesamt abgefragten IP-Adressen (rund 459 000 von 1351 000) nur ein einziges Mal in Erscheinung trat. Das berichteten Christian Dietrich und Christian Rossow vom Institut auf dem Heise-Cebit-Forum. Wenn ein Drittel aller beobachteten IP-Adressen nur ein einziges Mal Spam abfeuert, bedeutet das umgekehrt für Blacklists, die nur verifizierte, vor Kurzem beobachtete Spam-Quellen aufführen, eine Art „natürliche“ Obergrenze der Trefferquote von derzeit 66 Prozent.

Eine wesentliche Steigerung der „Einweg-Quote“ ist zurzeit nicht zu befürchten, denn IP-Adressen, die nur ein einziges Mal auftreten, lassen sich mit Greylisting wirksam blockieren. Dieses Verfahren geht davon aus, dass erwünschte Mails vor allem von Hosts stammen, die mehrmals in Erscheinung treten und anders als viele „Bots“ mit temporären Fehlermeldungen umgehen können.



Ein Tag auf der Blacklist: Sehr kurzlebige Adressen tauchen extrem häufig auf (blau, logarithmische Skala), und führen zu sehr wenigen Treffern (rot, rechte Skala).



WLAN und Roboter auf dem Vormarsch

Gut eingebettet

Christopher Kunz, Kersten Auel

Vom Spielerischen über Nützliches bis zu lebenserleichternden Anwendungen reichten die im Bereich Forschung auf der Cebit vorgestellten Projekte. Eine zunehmende Rolle in der IT spielen Erkenntnisse der Kognitionswissenschaften und der Hirnforschung.

Der Ausstellerschwund vergangener Jahre ging – ebenso wie das von der Messe AG mit vielen Vorschusslorbeeren bedachte neue Konzept – am in Halle 9 eingerichteten „Future Parc“ weitgehend vorbei. Wie gewohnt durch eine Mitteldiagonale von den in derselben Halle untergebrachten Dienstleistern für die öffentliche Hand getrennt, zeigten Universitäten und Forschungsinstitutionen ihre Neu- und Weiterentwicklungen des letzten Jahres. Neben wenigen Ständen ausländischer Universitäten fanden sich Spinoffs und Institute aus dem diesjährigen Partnerland Frankreich auf einem Gemeinschaftsstand ein. Die erdrückende Mehrheit der Exponate kam jedoch auch heuer aus Deutschland.

Neben den altbekannten Projekten aus dem Umfeld der Audio- und Videokodierung wartete der Stand der Fraunhofer-Gesellschaft mit einigen Neuerungen auf, darunter das Projekt „Hydra“. Der wenig vertrauenerweckende Name bezeichnet eine Middleware, die eingebettete Systeme zu einem intelligenten Gesamtnetzwerk verknüpfen und damit etwa das Gebäudemanagement erleichtern soll. Im augenfällig aus Plastikbauklötzen zusammengesetzten Beispielszenario zeigten die Entwickler vom Fraunhofer-Institut FIT, wie ein mit ihrem „Nervensystem“ ausgestattetes Haus feststellt, dass etwa die Heizung ausgefallen ist, selbstständig einen Techniker beauftragt und diesem eine temporäre Zutrittsberechtigung ausstellt. Die eingebetteten Überwachungssysteme dieses stark an „Big Brother“ erinnernden Szenarios stellen sicher, dass der Handwerker spätestens bis zum Ablauf der Autorisierung das Gebäude verlassen hat, andere Teile des Hausnetzwerkes beurteilen den Erfolg der Reparatur. Die Hydra-Middleware verwaltet sämtliche Komponenten des Netzes und vermittelt zwischen den je nach Hersteller und Verwendungszweck unterschiedlichen Zugangsprotokollen. So wollen die FIT-Wissenschaftler die Entwicklung von eingebetteten Systemen erleichtern und offene, klare Schnittstellen bereitstellen.



Quelle: Wissen Media Verlag GmbH, Gütersloh/München

Als „zeitgemäßes Infotainment“ versteht die Metaio GmbH die Verbindung klassischer Printmedien mit 3D-Inhalten (Abb. 1).

Ein anderes Projekt aus dem Fraunhofer-Institut IIS ist bestrebt, dem gerade in Städten allgegenwärtigen WLAN eine zusätzliche Funktion abzugewinnen. Für Umgebungen, die wegen dichter Bebauung für eine Positionsbestimmung über GPS nicht geeignet sind, hat das Erlanger Institut eine Alternative entwickelt und in der Innenstadt von Nürnberg erprobt. Zunächst legten sie dafür eine Signalkarte aller in der Stadt funkenden Access Points und deren Signalstärke an. Die Kombination aus der MAC-Adresse des AP und dessen Signalstärke dient hier als Unterscheidungsmerkmal.

Positionsermittlung in Sekundenschnelle

Eine für diverse mobile Endgeräte erhältliche Software ist nun, ausgestattet mit der zuvor angelegten Signalkarte, in der Lage, durch Triangulation zwischen den drei ihr am nächsten liegenden Zugriffspunkten ihre Position mit verblüffender Genauigkeit zu bestimmen. Im chronisch WLAN-übersättigten Cebit-Umfeld gelang ein erster Praxistest beim Standrundgang auf Anhieb. Selbst die vergleichsweise hohe Dynamik der Signalquellen – schließlich sind viele Hotspots nicht rund um die Uhr in Betrieb – beeinträchtigt die Lokalisierung nicht. Man habe beim Testbetrieb in Nürnberg festgestellt, dass bis zu 50 Prozent der kartierten APs ausfallen dürften, ohne dass die Genauigkeit der Ortsbestimmung gefährdet sei, so die Forscher. Wie punktgenau die WLAN-Lokalisierung funktioniert, ist trotzdem stark von den Umgebungsparametern abhängig: In einem geschlossenen Gebäude, das flächendeckend mit Access Points abgedeckt wird betrüge sie zwei bis vier, außerhalb von Gebäuden zwischen sieben und zwölf Metern.

Gegenüber dem Strom sparenderen Konkurrenten GPS hebt sich dieses Verfahren neben der Verwendbarkeit unter ungünstigen Bedingungen durch die deutlich schnellere initiale Positionsbestimmung hervor: Während ein GPS-Empfänger zur Ermittlung der Position durchaus eine Minute benötigt, beträgt die Antwortzeit per WLAN wenige Sekunden. Für die kommerziellen Anwendungen, die das IIS und seine Industriepartner konzipieren – etwa die Gelben Seiten und T-Systems –, ein schlagender Vorteil. Zielen die geplanten „Location based Services“ doch darauf ab, dem gestressten Stadtnomaden maßgeschneiderte Informationen aus seiner direkten Umgebung anzubieten.

An der TU Chemnitz forscht man mit ähnlichen Vorzeichen, aber anderen Ergebnissen. Hier werden ebenfalls existierende Techniken verwendet, um einen neuen Nutzen zu erzielen, allerdings richtet die Anwendung sich eher an Konferenzteilnehmer als an urbane Suchende. Die Forscher aus Sachsen haben ein drahtloses Konferenzsystem entworfen, das beim Anwender vorhandene Geräte einbezieht. Mit einer Software können die Besitzer WLAN-fähiger Endgeräte der über die drahtlose Schnittstelle übertragenen Simultanübersetzung bei internationalen Veranstaltungen lauschen. Für nicht derart technisierte Zeitgenossen besteht immer noch die Möglichkeit, mit Bluetooth-Headsets teilzunehmen – dort allerdings ist die Sprache vorbestimmt. Bis zu 50 Teilnehmer können mit jeder Sprachversion versorgt werden, die bisher hohen Kosten für Konferenzheadsets sollen so drastisch sinken. Die Chemnitzer hoffen auf reges Interesse aus der Wirtschaft.

Auf dem Stand des Bundesministeriums für Bildung und Forschung zeigte ein weiteres Fraunhofer-Institut, das FIRST, ein selbstlernendes Intrusion Detection System. Remind, so der Name des Produkts, ist anhand ausgeklügelter Verfahren aus dem Bereich des maschinellen Lernens in der Lage, bereits nach einer sehr kurzen Justierungsphase Angriffe selbstständig zu erkennen und zu melden oder zu unterbinden. Die von traditionellen IDS bekannten, ständig zu aktualisierenden Regelwerke sollen somit der Vergangenheit angehören (siehe auch Seite 26).



Anhänger dreidimensionaler Grafik konnten sich auf dem Stand der Hochschule Fulda an „Cloddy“ sattsehen. Die primär für Spiele konzipierte Grafik-Engine erlaubt einen praktisch beliebigen Detailgrad und gestattet dem Spieler so, aus dem Weltraum auf einen mit prozeduralen Verfahren modellierten Planeten zuzufliegen und ohne die in heutigen 3D-Spielen üblichen Übergänge auf diesem zu landen und in detaillierten Landschaften weiterzuspielen. Auch bereits existierende Landschaftsmodelle können problemlos mit Cloddy verwendet werden.

Bücher in neuen Dimensionen

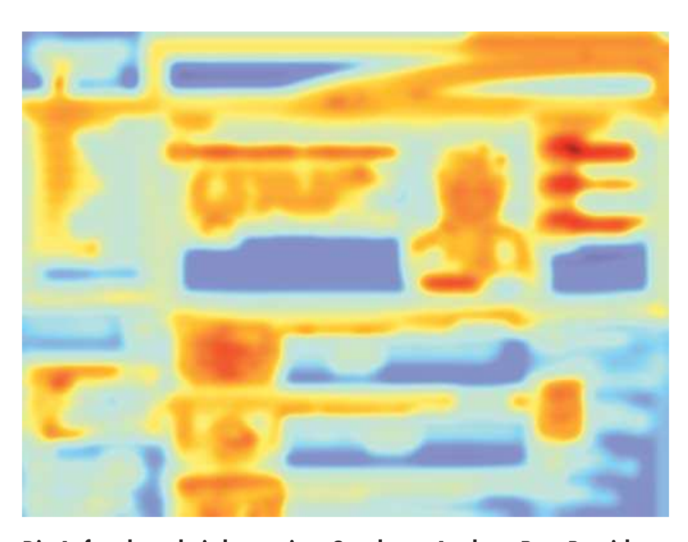
Wer neben dreidimensionalem Spielvergnügen ein gutes Buch zu schätzen weiß, dürfte sich für das „Augmented Reality Book“ der Metaio GmbH (www.metaio.com) interessieren, das am Stand des Bundesministeriums für Bildung und Forschung zu sehen war. Auch hier findet „Commodity“-Hardware, also bereits in vielen Haushalten vorhandene Technik, ein neues Anwendungsfeld. Die um Metaios Technik erweiterten Bücher enthalten an bestimmten Stellen einen Barcode. Um diesen zu erkennen, ist neben einem Laptop mit der Spezialsoftware eine handelsübliche auf das Buch gerichtete Webcam nötig. Die Software ordnet dem Barcode eine dreidimensionale Animation zu und spielt sie auf dem Laptop-Bildschirm ein. Der Leser soll so anschauliche Zusatzinformationen zu auf Papier schwer vermittelbaren Inhalten – etwa aus der Medizin oder Geografie – erhalten oder sich von lustigen Render-Figuren unterhalten lassen. Der Wissen Media Verlag (ein Unternehmen der DirectGroup Bertelsmann) will einen AR-Atlas bereits im Herbst dieses Jahres in den Handel bringen (siehe Abbildung 1).

Metaio setzt ihre Markertechnik bereits seit Jahren kommerziell ein. Auf der Cebit präsentierte die Firma unter anderem außerdem ein AR-Terminal. Der Benutzer hält eine Markerkarte in der Hand, und je nach ausgewählter Karte sieht er vor dem Monitor das 3D-Modell eines Autos von außen oder innen, kann es durch Bewegen der Karte drehen und kippen. Mögliche Einsatzgebiete sind Roadshows oder Ausstellungsräume von Händlern.

Roboter für fast alle Lebenslagen

Einen festen Platz auf der Cebit scheinen mittlerweile Roboter erobert zu haben. Die Computerlinguisten der Universität des Saarlandes präsentierten einen Prototyp mit einer Schnittstelle zu Lego Mindstorms, dem sie das Sprechen beigebracht haben (www.informatik-saarland.de). Der Roboter reagiert ohne Training auf gesprochene Anweisungen, antwortet, steuert auf Befehl Gegenstände an, greift sie und bringt sie dem Benutzer. Entwickelt wurde die Sprachsteuerungssoftware „Dialog OS“ von der CLT Sprachtechnologie GmbH, einem Spin-off-Unternehmen der Universität. Der sprechende Lego-Roboter ist für den Einsatz an Schulen konzipiert. Durch einen einfachen Nachbau beispielsweise ließe sich Schülern vermitteln, welche komplexen Aufgaben ein Computer lösen muss, wenn er menschliche Fähigkeiten wie Sprechen, Hören, Sehen oder Greifen nachahmen soll.

Mit künstlicher Intelligenz agiert der Roboter Zeno, der am neuseeländischen Gemeinschaftsstand in Halle 14 zu sehen war. Auf Basis der 3D-Animations- und -Simulationssoftware von Massive Software (www.massivesoftware.com), die dafür konzipiert ist, Bewegungsabläufe von Massenszenen zu realisieren – eingesetzt beispielsweise für „Der Herr der Ringe“ und „Ratatouille“ – nimmt Zeno, dessen Gehirn mit einem Computer verbunden ist, seine Umgebung wahr und kann darauf reagieren. Eine spezielle Software kontrolliert seine Reaktionen und ermöglicht es ihm, Schlüsse zu ziehen und dazuzulernen. Durch den Einsatz eines neu entwickelten, sich organisch anfühlenden Materials, mit dem das Gesicht des Roboters überzogen ist, lässt sich seine Mimik passend zu seinen verbalen Reaktionen steuern, sodass der Betrachter den Eindruck gewinnen kann, dass Zeno echte Gefühle ausdrückt. Angedacht ist, den Roboter sowohl in kleiner Ausführung als Spielzeug auf den Markt zu bringen als auch in einer größeren Variante für möglicherweise kommerzielle Zwecke. Ersteres eventuell noch in diesem Jahr.



Die Aufmerksamkeitskarte einer Goodgaze-Analyse: Rote Bereiche haben wahrscheinlich einen hohen Aufmerksamkeitswert, während blaue von vielen ignoriert werden (Abb. 2).

Einen „alltagstauglichen Rehabilitationsroboter“ hat das Institut für Automatisierungstechnik (IAT) der Universität Bremen entwickelt (www.iat.uni-bremen.de). Er soll es Personen mit schweren körperlichen Behinderungen erlauben, zumindest teilweise selbstbestimmt agieren zu können, statt rund um die Uhr auf die Hilfe anderer angewiesen zu sein. Amarob ist ein mit einem Leichtbauroboterarm und Greifer ausgestatteter Rollstuhl, mit dem man beispielsweise einem Kühlschrank Lebensmittel entnehmen kann. Die Ausführung der Aufgaben ist teilautonom, was bedeutet, dass der Benutzer in die Handlung eingreifen kann, wenn etwas schiefzugehen droht, falls das System beispielsweise durch veränderte Lichtverhältnisse die Lage des zu greifenden Gegenstandes nicht korrekt erkannt hat.

Hirnforschung in der IT

Für die Interaktion werden Eingabegeräte flexibel angekoppelt, die auf die individuelle Behinderung des Anwenders zugeschnitten sind. Dazu zählt unter anderem das Brain Computer Interface (BCI) des von der EU finanzierten Forschungsprojekts „Brainrobot“. Über die BCI-Schnittstelle lassen sich gemessene Gehirnsignale in Steuerbefehle für Hard- und Software umwandeln. Anders als bei anderen Schnittstellen dieser Art soll ein Training des Benutzers nicht notwendig sein (siehe auch Seite 30). Das System greift auf Bereiche des Gehirns zurück, die für die visuelle Wahrnehmung zuständig sind und misst die Synchronisation der Neuronen im visuellen Kontext beispielsweise mit der Frequenz einer blinkenden Lichtquelle, auf die die Konzentration des Benutzers gerichtet ist.

Die Blickrichtung und die Aufmerksamkeit eines Benutzers stehen auch im Zentrum des Projekts Goodgaze (www.goodgaze.de). Mitarbeiter des Instituts für Kognitionswissenschaft der Universität Osnabrück wollen anhand von in der Hirnforschung gewonnenen Erkenntnissen voraussagen, auf welchen Teil einer Website ein Anwender als Erstes blickt und welche Teile ihm am uninteressantesten erscheinen. Die Software soll als Webdienst angeboten werden. Goodgaze-Analysen, deren unmittelbar vorliegende Ergebnisse als Heatmaps visualisiert werden (Abb. 2), sollen den Designprozess einer Benutzeroberfläche direkt unterstützen. Eine Betaphase mit ausgewählten Benutzern soll direkt nach der Cebit begonnen haben. (ka)



Virtualisierungsforum auf der Cebit

Ohne doppelten Boden

Nikolai Zotow

Mit einem speziellen Forum, begleitet von einer mehrtätigen Vortragsreihe, lockte Magirus Besucher zum Thema Virtualisierung – ein etwas schwieriges Unterfangen wenige Tage nach der VMworld.

Eine Woche nach der VMworld in Cannes (siehe Beitrag auf Seite 40) hatte eigentlich niemand mit großen Neuigkeiten gerechnet. Trotzdem gab es eine echte Überraschung: Java Virtual Machines ohne ein Betriebssystem als virtuelle Instanz in VMwares Infrastructure 3 (VI3) zu betreiben, ist das Ziel der Allianz zwischen Bea und VMware. Die beiden Unternehmen arbeiten an einer Technik für die Anpassung der Laufzeitumgebung.

Es geht um die gemeinsame Entwicklung einer Schnittstelle, über die sich die JVM in den Hypervisor von VM-ware einklinken kann. BEAs LiquidVM (dev2dev.bea.com/liquidvm/vice/) liefert die Grundlage, eine spezielle Variante der JRockit VM für virtualisierte Umgebungen. VMwares Hypervisor in deren Virtualcenter enthält Erweiterungen, mit denen sich außerdem BEAs Weblogic Server Virtual Edition und andere Java-Applikationen autark als VMs einsetzen lassen.

IBMs Blades mit embedded ESX

Furore macht derzeit VMware ESX Server 3i, eine für den Einsatz mit Flash-Speichern abgespeckte Version des ESX Server. Zur VMworld hatten sich die Großen der IT – Dell, Fujitsu Siemens Computers (FSC), Hewlett-Packard, IBM, Sun und VMware – zusammengefunden und eine Vereinbarung getroffen, ESX 3i on board zu integrieren. Zur Cebit präsentierte IBM dann seinen Blade-Server HS21 XM im Bladecenter mit VMware ESX Server 3i, zu booten aus dem 4 GByte-Flash einer speziellen Zusatzkarte (siehe Abbildung). Mit dabei ist IBMs Director.

Der Blade-Server HS21 XM (www-3.ibm.com/systems/bladecenter/hardware/servers/hs21xm) läuft mit Intels bis zu 3 GHz schnellem Dual- oder Quad-Core-Xeon-Prozessor. IBM hat ihn für bis zu 32 GByte RAM ausgelegt, im Unterschied zu seinem Pendant HS21, das ohne Erweiterung nur 16 GByte Hauptspeicher verkraftet. Maximal vier SAS-Platten (je 146 GByte) in einer zusätzlichen SIO-Blade stellen gut ein halbes Terabyte Massenspeicher bereit. Der Server nutzt wie die Rack-Systeme vom Typ System x 3850 M2 die vierte Generation des Chipsatzes eX4 (www-03.ibm.com/systems/x/hardware/enterprise/x3850m2/ex4), die ebenfalls mit eingebautem ESX Server 3i auf den Markt kommen soll.



Blitzschnell: Wer VMwares Hypervisor zur Virtualisierung nutzen will, muss ihn bei IBMs Blade-Server HS21 XM nicht erst installieren – der ESX Server startet aus dem Flash-Speicher.



Flache Flunder oder kleine Wunder

Sein ultraflaches Thinkpad X300 hat Lenovo zur Cebit auf dem Freigelände bei Vodafone D2 vorgestellt und will damit gegen Apples Macbook Air antreten. Der mit einem Intel Core 2 Duo ausgestattete Rechner verfügt über bis zu 4 GByte RAM und eine 64 GByte große Solid State Disk (SSD). Der X300 besitzt die beim Thinkpad üblichen Sicherheitsmerkmale wie einen Fingerabdruckleser, eine Funktion zum Deaktivieren der Ein-/Ausgabe und einen 32-Byte-Kennwortschutz. Anders als das Macbook Air ist der 300x mit einem optischen Laufwerk erhältlich. Lenovo und Apple haben zwar einen ähnlichen Formfaktor, doch das X300 ist vor allem für Geschäftsleute gedacht und mit 2500 Euro erheblich teurer als das Air.

Auf dem Stand von Asus gab es den Eee PC 4G (siehe Beitrag auf Seite 87) zu sehen. Der Hersteller nutzte die Messe dafür, seine Kooperation mit T-Mobile und Microsoft für das Subnotebook bekanntzugeben. Den Mini-Laptop, den es bislang nur mit einer Linux-Distribution von Xandros gab, erhält man nun wahlweise mit Windows XP; enthalten sind Microsoft Works, Windows Live, ein Internetzugang (Excellent Internet) sowie mobile Unterhaltung (Entertainment on the Go). Die größere Variante EeePC 900 mit 8,9 Zoll großem Bildschirm (1024 × 600) und 1 GByte RAM soll ab Sommer voraussichtlich für 400 Euro erhältlich sein.

Von T-Mobile kommen die Pakete mit 300 Hotspot-Freistunden, die zukünftig beim Kauf eines EeePC für 299 Euro enthalten sind. Das Angebot gibt es vorerst nur in Deutschland und Österreich. Weitere Angebote für das mobile Internet soll es noch im Jahr 2008 geben: USB-Sticks für UMTS und HSDPA.

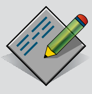
Toshiba stellte eine Designstudie vor, die in einem Gerät Multimediawiedergabe, Navigation, mobiles Internet und andere Funktionen vereint. Der Rechner lief bei der Demonstration unter Vista Ultimate. Er besitzt keine mechanische Tastatur, sondern emuliert das Keyboard auf dem berührungsempfindlichen Bildschirm.

Nikolai Zotow



Tastenlos: Ganz ohne mechanische Tasten kommt das Notebook aus, das Toshiba als Studie auf der Cebit zeigte. Das „virtuelle" Keyboard kann man über den Touchscreen bedienen.

KURZ NOTIERT



Gewusst wo: Garmin Mobil PC verwandelt Notebooks in ein Navigationsgerät. Die Software, die es nur für Windows gibt, nutzt per Bluetooth oder Kabel angeschlossene GPS-Empfänger und soll ab April für 70 Euro zu haben sein (www.garmin.de).

Unterboten: Ein 269 Euro teures Subnotebook mit Linux zeigte der Grafikkartenhersteller GeCube auf der Cebit. Er besitzt ein abnehmbares, 7 Zoll großes Display mit 800 × 480 Bildpunkten, wiegt 950 g, hat die Maße 23 × 14,6 × 3,3 cm und kommt laut Hersteller mit einer Akkuladung bis zu 3,5 Stunden aus (www.gecube.com/products.php?lang=de).

Übern Berg: Intels nächste Mobilplattform Centrino 2 (Projektname Montevina) spendiert den Core-2-Duo-CPUs mit FSB1066 einen schnelleren Frontside-Bus als die Vorgängerin (Santa Rosa). Die Northbridge GM45 erlaubt den Einsatz von DDR3-RAM und soll eine höhere Grafikleistung bringen (www.intel.com).

Neue Produkte sollen Verlust vertraulicher Daten in Unternehmen verhindern

Nicht erst seit dem jüngsten Steuerskandal ist der Begriff „Data Leakage Prevention" (DLP) – das Verhindern unerwünschter „Datenabflüsse" in Unternehmen – in aller Munde. Auch auf der Cebit stellten einige Hersteller aus der Sicherheitsbranche diesbezügliche Produkte vor.

Verschlüsselungsspezialist PGP (www.pgp.com) hat sich mit Lumension (vormals Secuwave), Hersteller von auf Whitelists basierenden Applikations- und Device-Kontrollprodukten, zusammengetan. Dessen Produkte sollen bis zum Mai in die PGP-Suite integriert sein. Ziel ist die sogenannte Endpoint-Security, das heißt auf den Endgeräten soll jeglicher Datentransfer und -fluss kontrolliert, gegebenenfalls blockiert und eine Verschlüsselung erzwungen werden können. Das gemeinsame Produkt firmiert unter PGP, soll aber auch von der Lumension-Konsole aus zentral verwaltbar und für Großunternehmen einzusetzen sein.

Ebenfalls neu in der DLP-Branche ist Trend Micro (www.trendmicro.com). Dessen „Leak Proof", bestehend aus Softwareagenten für die Clients und einem Fingerprintserver (als Hardware- oder virtuelle Appliance), setzt den Schwerpunkt auf das Verhindern des versehentlichen Verlusts oder Verschickens sensibler Daten. Die Erkennung vertraulicher Dokumente soll selbst beim Umkopieren oder Aufteilen in kleinere Teile (bis zu 30 % des Originals) noch funktionieren. Trend Micro will das von Provilla aufgekaufte Produkt hinsichtlich „Look & Feel" und Verwaltbarkeit in die eigene Produktreihe integrieren.

Für sein DLP-Produkt „Total Protection for Data" arbeitet McAfee (www.mcafee.com) mit dem Verschlüsselungshersteller Safeboot zusammen. Das Werkzeug beruht zum einen auf Schnittstellenblockierung und zum anderen auf der Kontrolle der Datenbewegungen mittels Markierung (Tagging) der Daten. Die durch Richtlinien erzwingbare Verschlüsselung stammt von Safeboot. Neu in Version 2.1. ist die separate Lizenzierung des Device Blocking sowie die Unterstützung des Managementwerkzeugs ePolicy Orchestrator.

Der Verlust vertraulicher Daten beschäftigt auch das diesjährige Cebit-Partnerland Frankreich. „Digital DNA" nennt der französische Hersteller Mobilegov (www.mobilegov.com) seine Methode der Erfassung und Markierung von Hardware-Devices, die an ein definiertes Netz angeschlossen werden dürfen. Die „Device Authenticator Pro Edition" überprüft außerdem die Konfigurationszustände der angeschlossenen Datenträger und leitet bei Veränderung Maßnahmen ein. Der „Device Linker" soll gewährleisten, dass USB-Sticks nur an autorisierte Geräte angeschlossen werden können. Stöpselt ein Angestellter seinen Stick etwa am heimischen PC ein, sind die Daten dort nicht zugänglich. Die Produkte werden in Kürze auch in Deutschland erhältlich sein.

Auch Ironport (www.ironport.de), Prosoft (www.prosoft.de), Utimaco (www.utimaco.de), Websense (www.websense.de), Infowatch (www.infowatch.com/de) und Tetraguard (www.tetraguard.de) zeigten ihre Produkte zur Verhinderung von Datendiebstahl.

Selbstlernendes Intrusion-Detection-System

Die enorme Anzahl und Größe von Software-Updates wird zukünftig kaum mehr zu managen sein, so das Fraunhofer Institut Rechnerarchitektur und Softwaretechnik (FIRST, www.first.fraunhofer.de). Es hat daher auf der Basis des maschinellen Lernens ein selbstlernendes Intrusion-Detection-System (IDS) namens „Remind" entwickelt, das keine Aktualisierungen benötigt. Ausgehend davon, dass ein Angreifer sich anormal verhalten muss, um in ein System einzudringen, analysiert Remind Ereignisse (Verbindungen, Protokolle et cetera), splittet sie auf und stellt sie geometrisch dar. Aus dem Abstand zwischen diesen dargestellten Punkten lässt sich schließen, ob die Software schädlich ist oder nicht. Denn da sich alle schädlichen Programme ähnlich verhalten und auch alle nicht schädlichen, haben die Programme einer Kategorie zueinander einen geringen, aber zur anderen Kategorie einen großen Abstand. Mit dieser Methode kann man laut Aussage von FIRST 90 % der unbekannten Angriffe erkennen. Zur Einführung in die Materie hat das Institut einen originellen animierten Film erstellen lassen, der nun auf Youtube öffentlich verfügbar ist (www.youtube.com/watch?v=6Sm2-klwTUs).



Drei Sicherheitswerkzeuge von Microsoft

Zur Cebit stellt Microsoft gleich drei Werkzeuge vor, die Unternehmen bei der Entwicklung sicherer Anwendungen und der Umsetzung von Sicherheitsanforderungen und -richtlinien helfen sollen. Zwei von ihnen, „CAT.Net", das der Code-Analyse dient, sowie eine Software für „Threat Analysis & Modeling", waren bislang nur im internen Gebrauch bei der Softwareschmiede. Ein drittes, ein Audittool namens Spider, wurde neu entwickelt.

CAT.Net ist angesiedelt zwischen den herkömmlichen Penetrationstestwerkzeugen, die automatisiert Angriffe auf Applikationen fahren, und dem manuellen Untersuchen des Anwendungs-Sourcecodes auf potenzielle Einfallstore durch den Sicherheitsexperten.

Das Werkzeug soll den Prozess des manuellen Code-Analysierens automatisiert unterstützen. Dabei sucht es nach häufigen sicherheitsrelevanten Programmierfehlern, die Angriffe auf Applikationsebene wie Cross-Site Scripting, SQL Injection, XPath Injection oder LDAP Injection ermöglichen. Es analysiert, wie das untersuchte Programm die Eingabedaten behandelt.

Die Software für „Threat Analysis & Modeling" soll Projektmanagern und Teamleitern von Entwicklungsabteilungen helfen, Bedrohungsszenarien zu modellieren und dafür Verantwortlichkeiten zu definieren. Überdies soll sie bei der Umsetzung der Sicherheitsziele bei der Softwareerstellung helfen. Wenn beispielsweise die Richtlinie eines Unternehmens die Verschlüsselung von Kundendaten zwingend vorschreibt, hilft die Software den Projektverantwortlichen, dieses Ziel nicht aus den Augen zu verlieren.

Das dritte Werkzeug, die Auditsoftware Spider, überprüft die sicherheitstechnischen Richtlinien innerhalb eines Unternehmens – Stichwort Compliance. Mithilfe der Berichts- und Darstellungsfunktion von Microsofts SQL Server soll Spider Manager über die Erfüllung dieser Vorgaben unterrichten und sie bei weiteren Entscheidungen unterstützen. Alle drei Werkzeuge behandeln jedoch nur einen Teil des „Security Development Lifecycle for IT", darauf weist Microsoft ausdrücklich hin. Sie sind ab sofort bei Microsoft selbst sowie bei zertifizierten Partnern erhältlich.

IT-Experten sind Mangelware

Starke Nachfrage

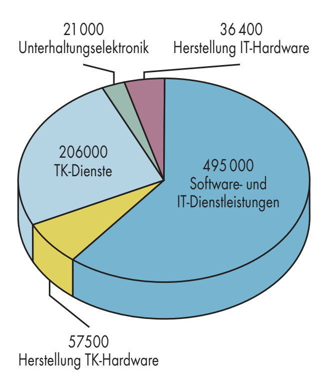
Achim Born

Äußeres Zeichen für den Charakter der Cebit als größte branchenspezifische Job- und Kontaktbörse der Welt waren die Ausweitung der Aktivitäten, Ausstellungen und Kongresse rund um das Thema „Ausbildung und Beruf“.

Das Wachstum in der ITK-Wirtschaft hinterlässt Spuren im Arbeitsmarkt. Bereits auf ihrer Pressekonferenz am Vormessetag verkündete der Bitkom die Ergebnisse seiner jüngsten Statistik. Danach ist die Zahl der Erwerbstätigen in der ITK-Branche im vergangenen Jahr um 3000 auf 816 000 gestiegen. Allein Softwarehäuser und IT-Dienstleister sollen im vergangenen Jahr 17 000 zusätzliche Stellen geschaffen haben. Damit gelang es, die Entlassungen in einigen großen Unternehmen mehr als auszugleichen. Laut Bitkom-Präsident Prof. August-Wilhelm Scheer wäre der Stellenzuwachs höher ausgefallen, wenn offene Stellen schneller hätten besetzt werden können. 43 000 freie Stellen für IT-Spezialisten, davon 18 000 im ITK-Sektor, soll es seinen Angaben zufolge geben. Jedes vierte ITK-Unternehmen musste im vergangenen Jahr zudem Aufträge ablehnen, weil es die notwendigen Mitarbeiter nicht finden konnte. Selbst wenn es sich dabei in einigen Fällen um doppelte Ausschreibungen gehandelt haben kann, verliert die Aussage im Kern nicht an Brisanz. Scheer ist deshalb überzeugt: „Qualifizierte Mitarbeiter finden und binden ist neben der Green IT das bestimmende Thema dieses Jahres.“

Die Cebit-Macher bemühten sich, dem vorauseilenden Ruf als größte branchenspezifische Job- und Kontaktbörse gerecht zu werden. Beispielsweise legte allein die Ausstellungsfläche des traditionell in Halle 6 angesiedelten „Job & Career Market“ um 50 % zu. Unternehmen aus nahezu allen Branchen, von klassischen IT-Firmen wie der Dortmunder Materna (200 offene Stellen) bis hin zum Lebensmitteldiscounter Lidl, buhlten hier um das Interesse der Besucher. Neben Absolventen kamen dabei dem Vernehmen nach durchaus die händeringend gesuchten IT-Profis mit Berufserfahrung vorbei, um sich über Angebote zu informieren und/oder den Marktwert zu bestimmen.

In Sachen Entgelt vermittelt die Branche allerdings zurzeit kein eindeutiges Bild. Während etwa eine gemeinsam von der Computerwoche und der Vergütungsberatung Personalmarkt durchgeführte Analyse durchaus Gehaltssteigerungen aufspürte, kommt die IG Metall zu einem gänzlich anderen Schluss. In der bereits zum zehnten Mal anlässlich der Cebit veröffentlichten ITK-Entgeltanalyse heißt es im Ergebnis lapidar, dass die meisten Jobgruppen bislang nicht vom positiven Wirtschaftstrend der Branche profitiert haben. (WM)

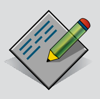




IBM stellt Cognos-Strategie vor

Nach Abschluss der Übernahme des Business-Intelligence-Anbieters Cognos zeigte IBM erste gemeinsame Ergebnisse. Dazu gehören zehn Branchensoftwarepakete etwa für Banken, Einzelhandel, Gesundheitswesen sowie verarbeitende Industrie. Zudem sechs vorkonfigurierte BI-Produkte, beispielsweise ein Cognos 8 Starter Pack für das Infosphere Warehouse, eine vorkonfigurierte Version für die hauseigene Information-Server-Plattform und Vorlagen für die Integration von Cognos 8 BI in die Business-Process-Management-Software von Filenet. Mit neuen Dienstleistungen rund um das Bereitstellen von Informationen im Unternehmen sowie der Gründung einer Community, in der sich die Benutzer der BI-Software austauschen sollen, will IBM seine diesbezügliche Strategie abrunden.

KURZ NOTIERT



Bildhaft: Die neuseeländische Firma Centruflow hat die Version 3.0 ihrer Kollaborationssoftware vorgestellt. Sie soll für das Unternehmen wichtige Informationen grafisch, bebildert und leicht verständlich darstellen. Laut Centruflow lassen sich viele Fehlentscheidungen auf schlecht aufbereitetes und unverständliches Datenmaterial zurückführen (www.centruflow.com).

Klare Prozesse: Touchpaper hat seine Business-Management-Suite in der Version 7.2.3 mit vorgefertigten Funktionen für die Personalverwaltung angereichert. Sie sollen Standardprozesse wie Einstellung und Kündigungen übersichtlich abbilden. Ein neues Toolkit erleichtert die Integration von Touchpapers Service-Desk-Komponente in eigene Anwendungen.

Prozessgeschichte: Seiner Dokumentenverarbeitungssoftware Beta UX hat das gleichnamige Berliner Softwarehaus neue Funktionen spendiert. Sie beherrscht nun das Archivformat PDF/A sowie das History-Management von Rechenzentrumsprozessen. Dazu wertet die Software alle bereitgestellten Protokolle aus und bietet die Möglichkeit, die Vorgänge zentral zu bearbeiten und zu archivieren.

SOA-Buch: Unter dem Titel „SOA für agile Unternehmen – Serviceorientierte Architekturen verstehen, einführen und nutzen“ erscheint im April ein Ratgeber im Verlag Symposion Publishing. Zielgruppe sind Geschäftsführer und IT-Verantwortliche. Im Vordergrund steht der Nutzen von SOA für das Unternehmen.

ERP light: Intersystems zeigte eine neue Version seiner Mittelstands-ERP-Lösung cierp3. Die reine Webanwendung bekam zudem einen vorkonfigurierten Ableger namens cierp3 easy, mit dem maximal fünf Benutzer gleichzeitig arbeiten können. Angeblich lässt sich das ERP-System über Webschnittstellen leicht mit anderen Webapplikationen wie Onlineshops oder B2B-Portalen zusammenführen.

Prozessbündel: Unter dem Namen „Aris Business Performance Edition“ hat IDS Scheer eine Reihe neuer und bekannter Produkte zusammengefasst, mit denen der Anwender Geschäftsprozesse, die Nutzung von IT-Systemen sowie das Management gesetzlicher und vertraglicher Belange (Compliance) verbessern kann. Beispielsweise enthält die Edition Funktionen für die Überwachung unterschiedlicher Prozessversionen.

Service-Trip: Der Karlsruher Softwareanbieter Abas hat seine ERP-Software für den Wartungsbetrieb ausgeweitet. Alle relevanten Daten zum Serviceauftrag kann der zuständige Techniker im Internet abrufen und bearbeiten. Die Oberfläche ist so angelegt, dass die Bedienung per Touchscreen möglich ist. Über einen integrierten Webshop lassen sich Ersatzteile bestellen.

SAP: Verdienen in allen Bereichen

Verdienen möchte SAP weiterhin mit Unternehmen aller Größenordnungen. Selbst im Großkundengeschäft sieht man immer noch gute Absatzchancen. Für die Messe stellten die Walldorfer jedoch ihre Mittelstandsangebote in den Vordergrund. Besonderes Augenmerk galt den Paketen rund um Business All-in-One, das im Unterschied zu den weiteren Offerten für die Kleinen und Mittleren (Business One und das SaaS-Produkt Business By Design) auf derselben Codebasis läuft wie die große SAP-Lösung.

Mit Aris Smartpath führte IDS Scheer mittelständischen Firmen eine prozessorientierte Anwendung auf Grundlage von Business All-in-One vor. Steeb brachte ein voreingestelltes Paket einschließlich Kontaktleitstand mit. T-Systems wiederum bewarb Dynamic Services for SAP Solutions. Hierbei erfolgt der Betrieb von Mittelstandssoftware nach einem dynamischen Modell mit Abrechnung nach beauftragter Leistungsmenge.

Zu den wirklichen Neuheiten im Umfeld von Business All-in-One zählte der gemeinsam mit Intel gebaute Prototyp eines vorkonfigurierten SAP-Servers, angetrieben durch Xeon-Quadcore-Technik. Geplant ist, die Programme mit Suse Linux Enterprise sowie SAPs Datenbank MaxDB auf Serversystemen von Intels OEM-Partnern gebrauchsfertig zu installieren. Angeblich betreiben mehr als 700 mittelständische Firmen ihre SAP-Anwendungen unter Linux, davon rund 35 % in Kombination mit MaxDB.

Verhältnismäßig wenig Aufhebens machte das Management um Business By Design. Mittlerweile hat man laut eigenem Bekunden in Deutschland 70 Kunden für die Mietsoftware gewonnen. Zudem wollen 21 neue sogenannte Early Partners aus Deutschland, England, Frankreich und China die Markteinführung unterstützen. Zu 16 von ihnen unterhält SAP allerdings schon Partnerschaften für Business One oder Business All-in-One. Zu den fünf Neulingen zählen Alpha Business Solutions, GUS und Portolan aus Deutschland sowie Mynet und Inventec aus China. Einige Namen auf der Liste gaben Anlass zum Schmunzeln. Denn Unternehmen wie GUS pflegten in der Vergangenheit zumindest eine verbale Konkurrenz zur übermächtigen SAP.

Reddot integriert Web-2.0-Funktionen

Erste Einblicke in die kommende Generation seiner Web Solutions Suite gewährte Reddot. Anfang 2007 übernahm Open Text, Anbieter von Enterprise-Content-Management-Produkten, das deutsche Unternehmen. Es verantwortet als eigenständiger Bereich das komplette Webgeschäft. Die ab Sommer erhältliche Suite hat man vor allem mit sogenannten Social-Computing-Komponenten wie Wikis, Foren, Blogs, Onlinegemeinschaften und Echtzeit-Zusammenarbeitsfunktionen angereichert. Zudem kooperiert Reddot mit dem auf SAPs Netweaver-Portale spezialisierten Beratungshaus Btexx. Man will die bestehenden Portal-CMS-Lösungen zusammenführen, gemeinsam weiterentwickeln und unter der Marke Reddot vertreiben.

CRM im Mietmodus von CAS

CRM-Anbieter CAS hat ein SaaS-Paket (Software as a Service) speziell für kleine Firmen mit bis zu 20 Arbeitsplätzen geschnürt. Laut Hersteller handelt es sich bei dem Produkt um eine komplette Neuentwicklung, die technisch auf Eclipse RAP (Rich Ajax Platform) basiert. Neben den üblichen Groupware-Funktionen (Kalender, Aufgaben, Wiedervorlagen) enthält das Angebot eine digitale Kundenakte. Ebenso zum Lieferumfang gehören Funktionen für das Management von Kampagnen, Dokumenten und Verkaufschancen. Laut CAS können die Kunden das Onlineprogramm, das auch über mobile Endgeräte zu bedienen sein soll, ab Sommer nutzen. Preislich will man die Konkurrenz weit unterbieten.



Gesetzeskonforme digitale Unterschrift

Viele Stiche

Christian Kirsch

Im elften Jahr nach der Veröffentlichung des ersten Signaturgesetzes sollen Gesundheitskarte, Personalausweis und eine einheitliche API der digitalen Signatur mal wieder den Durchbruch bringen.

Pünktlich zur Cebit stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI, www.bsi.de) die sogenannte eCard-API vor. Sie soll Anwendungsentwicklern die Einbindung digitaler Signaturen erleichtern, indem sie sie vor den unterschiedlichen Betriebssystemen der Smartcards und der Plattformen abschirmt. Konfigurationsdateien („Cardinfo Files“) definieren in diesem Modell kartenspezifische Details und bringen Flexibilität: Neue Karten sollen mit vorhandenen Programmen benutzbar sein.

Vorrangiges Ziel bei der Entwicklung der API war der Einsatz in vernetzten Umgebungen, etwa bei der geplanten elektronischen Gesundheitskarte (eGK). Deshalb liegt sie bislang ausschließlich in Form einer WSDL-Beschreibung (Web Services Description Language) vor. Fertige Bindings für C, C++ oder Java gibt es noch nicht. Aus den WSDL-Daten sollen sich jedoch nach Auskunft von Beteiligten mit geeigneten Werkzeugen Java-Schnittstellen generieren lassen.

Der Funktionsumfang geht weit über das hinaus, was man für (qualifizierte) Signaturen am Client braucht. So regelt die API die Kommunikation zwischen den Smartcards von Arzt und Patient ebenso wie das transparente Signieren von fernen Anwendungen aus.



Auf der microSD-Karte von Certgate lässt sich ein qualifiziertes Zertifikat unterbringen.

Funktionstests erst später

Eine erste Implementierung der eCard-API will Openlimit (www.openlimit.com) bald anbieten. Unter Sicherheitsgesichtspunkten kann das BSI sie bereits jetzt zertifizieren. Funktionstests gibt es jedoch noch nicht; die Behörde will sie innerhalb von sechs Wochen erstellen. Die gesamte API-Definition steht auf www.bsi.de/literat/tr/tr03112 bereit.

Die Certgate GmbH (www.certgate.com) zeigte ihre microSD-Karte mit integriertem Krypto-Prozessor. Sie lässt sich mit einem qualifizierten Zertifikat bestücken und so zum Beispiel in einem Handy zum gesetzeskonformen Unterschreiben verwenden. Eine Anwendung zeigte die Firma gemeinsam mit dem Informatikzentrum der Sparkassen (www.siz.de). Sie ermöglicht Geschäftskunden im EBICS-Verfahren (Electronic Banking Internet Communication Standard), Überweisungen am mobilen Gerät zu signieren. Zielgruppe sind Firmen, die mehrere Signaturen für bestimmte Zahlungsaufträge verlangen. Mit der microSD-Karte können Unterschriftsberechtigte auch unterwegs das Nötige erledigen. Einen anderen Einsatz demonstrierte die Schweizer Esiqia AG, die die Karte in einen am Arm tragbaren Mini-Rechner integriert. Damit lassen sich etwa bei der Flugzeugwartung Dokumente während der Arbeit unterzeichnen. (ck)



Gesundheitskarte: „Aufhören, über Schlüssellängen zu diskutieren“

In den Startlöchern?

Susanne Schwonbeck

Selten war die Stimmungsdiskrepanz zwischen Befürwortern und Gegnern der elektronischen Gesundheitskarte so groß wie im Moment. Während Ärzte über mangelnde Aufklärung klagen und Datenschutzbedenken anmelden, scharren die Hersteller ungeduldig mit den Hufen.

Cebit-Besucher fanden in diesem Jahr die Internationale Kongressmesse für ICT-Lösungen im Gesundheitsmarkt „Telehealth“ zum ersten Mal in die IT-Messe integriert. Laut Veranstalter war das Besucherinteresse deutlich größer als im vergangenen Jahr, was sicher nicht zuletzt an dieser neuen Positionierung der zweitägigen Veranstaltung liegt. 53 Aussteller aus insgesamt neun europäischen Ländern präsentierten Produkte, Anwendungen und Pilotprojekte aller Art in Halle 8.

Während der Messe fand ein Kongress statt, der sich in Firmenvorträge, Workshops, Podiumsdiskussionen und Symposien in zwei parallelen Foren gliederte. Ein netter Zug der Veranstalter war die Synchronübersetzung von und ins Englische sowie die Ausgabe von Kopfhörern an das Publikum. Das war auch nötig, da das diesjährige Cebit-Partnerland Frankreich in einem Symposium zum Thema E-Health zu Wort kam.

Allgegenwärtig und heiß umstritten war das Thema elektronische Gesundheitskarte (eGK). So zeigte die Gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, www.gematik.de) – die nach SGB V § 291b für die Einführung der eGK verantwortliche Gesellschaft – insgesamt achtmal an ihrem Demonstrationsstand, wie Patienten in Zukunft mit ihrer Gesundheitskarte beim Arzt, in der Apotheke und am geplanten Informationsterminal umgehen können. Laut Auskunft der Gematik soll Ende 2008/Anfang 2009 die Online-Testphase der eGK in sieben ausgewählten Modellregionen (Baden-Württemberg, Bayern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen und Schleswig-Holstein) mit 10 000 freiwilligen Patienten beginnen.

Infrastruktur noch unvollständig

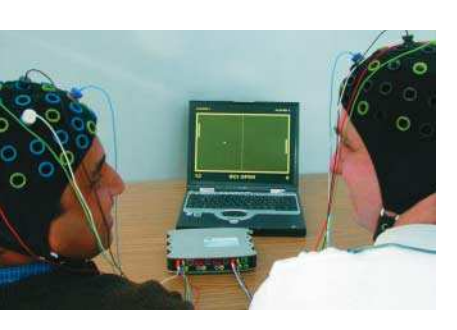
Größtes Hindernis bei der Einführung und auch Grund für die bisherige Verzögerung ist die noch fehlende beziehungsweise unvollständige Telematik-Infrastruktur. Einige Ärzte oder Praxen sind bisher nicht in das System eingebunden. Noch immer mangelt es an Aufklärung, noch immer ist der Widerstand seitens der Beteiligten groß. Das zeigte sich deutlich bei der Podiumsdiskussion mit dem Titel „Chancen der Telemedizin im Gesundheitswesen“, an der unter anderem Vertreter der Bundesärztekammer, der Gematik sowie der Deutschen Angestellten Krankenkasse (DAK) teilnahmen.

So forderte einerseits Claus Moldenhauer von der DAK: „Wir brauchen die eGK, um die Sicherheit der Patienten zu gewährleisten“, während Philipp Stachwitz von der Bundesärztekammer vor permanenter Datenerhebung, Problemen bei Verschiebungen ärztlicher Fachbereiche, dem Datenlöschungsrecht der Patienten und den daraus resultierenden Haftungsproblemen warnte. Darüber hinaus ist noch immer nicht geklärt, wer die Kosten für die neue Infrastruktur übernimmt.

Demgegenüber reicht die Stimmung bei den Ausrüsterfirmen vom entspannten „wir sind bereit“ bei Atos Worldline (www.atosworldline.com) bis zum „man sollte aufhören, über Schlüssellängen zu diskutieren, und stattdessen anfangen, Karten und Terminals auszugeben“ von Andreas Lösch von der Gemalto GmbH. Trotz solch deutlicher Worte und der geplanten Pilottests bleibt offen, wann genau 80 Millionen Bundesbürger mit der Ausgabe der eGK rechnen müssen. (ur)

Softwaresteuerung via Gehirn

Dauerumlagert war auf der Cebit der Stand der österreichischen Firma g.tec (www.gtec.at), die ihr Gehirn-Computer-Interface BCI vorstellte. Gemeinsam mit der von g.tec entwickelten Software g.RTsys und g.RTanalyze erlaubt das „Brain Computer Interface“ eine Computersteuerung mittels Elektroenzephalografie (EEG). Die Entwickler konnten in der neuen Version die Zeit von 10 Stunden auf fünf Minuten reduzieren, die für das Training der Software notwendig waren. Viele Messebesucher probierten das Buchstabieren per Gehirnwellen aus. Das Gerät ist nun durch den Einsatz von Bluetooth vollständig mobil.



Der Hersteller sieht sein Produkt als Alltagshilfe für gelähmte Patienten, die so beispielsweise schreiben, eine entsprechend ausgerüstete Umgebung steuern (Anschalten von Fernseher, Musikanlage, Licht) oder mit dem Computer kommunizieren können. Eine weitere Anwendung ist die Bewegung in virtuellen Räumen durch ausschließliche Gedankenkontrolle. Je nach Ausstattung ist das Gerät samt Software und Verstärker für 4000 bis 80 000 Euro erhältlich.

Susanne Schwonbeck

Schlaf, Bienchen, schlaf ...

Das Fraunhofer Institut Photonische Mikrosysteme IPMS (www.ipms.fraunhofer.de) präsentierte das mobile Schlaf-Diagnose-System „Sleepbee“. Statt der in stationären Schlaflaboren üblichen Totalverkabelung besteht das System aus Sensoren und Signalverstärkern, die man direkt am Körper des Schlafpatienten befestigt. 14 Signale (darunter EEG, Atmung, EMG, Schnarchen) werden per Funk an eine neben dem Bett befindliche Basisstation übertragen und auf einer SD-Karte gespeichert. Damit können Patienten auch im eigenen Bett eine Schlafdiagnose durchführen, statt endlos auf der Schlaflabor-Warteliste zu stehen. Das IPMS sucht nun Partner aus der Industrie, um Sleepbee weiterzuentwickeln. *Susanne Schwonbeck*

Unterstützung bei Arzneimittelverordnung

Eine Weiterentwicklung ihrer modularen Software zur elektronischen Verordnungsunterstützung „Rpdoc“ zeigte die Rpdoc Solutions GmbH (www.rpdoc.de). Das für den Krankenhausbetrieb konzipierte Programm greift über XML auf Patientendaten und bereits vorliegende Laborbefunde zu und weist das behandelnde Personal im Falle von unerwünschten Wechselwirkungen der verordneten Arzneimittel auf potenzielle Gefahren hin. Das Programm enthält außerdem eine Schnittstelle für die Patientenidentifikation per RFID. *Susanne Schwonbeck*



Zusammenarbeit gesetzlich verankern

Sanfte Zwänge

Barbara Lange

Die öffentlichen Verwaltungen sollen ihre Prozesse vereinheitlichen, serviceorientiert und wirtschaftlich arbeiten sowie einheitliche Ansprechpartner stellen. Genug Diskussionsbedarf für den Public Sector Parc.

Wie im vergangenen Jahr eröffnete Bundesinnenminister Schäuble den Public Sector Parc in Halle 9. E-Government könne nicht mehr von einzelnen Behörden und Ressorts umgesetzt werden, sondern nur ressort- und ebenenübergreifend, was letztlich auch durch die Etablierung des Bundes-CIO Ende vergangenen Jahres deutlich wurde, so der Minister. Noch dauere die Einführung von IT-Systemen in den Verwaltungen oft viel zu lange – und einmal eingeführt, sind sie oft aufgrund der hohen Innovationsgeschwindigkeit schon wieder überholt.

Daher, so Schäuble, sei ein „angemessener Rechtsrahmen“ erforderlich, der die bundes- und länderübergreifende Zusammenarbeit von Behörden als Pflicht definiert. Wie bereits im letzten Jahr deutete er an, diese Pflicht auch im Gesetz verankern zu wollen. Dabei ginge es nicht um die Abschaffung von Föderalismus, sondern um eine „vernünftige“ Zusammenarbeit.

Darüber hinaus betonte er die Bedeutung der IT-Sicherheit und warnte vor der Verletzbarkeit der IT-Infrastrukturen, die die Staaten auf ganz neue Art anfällig machen würden. Vor diesem Hintergrund forderte er die Hersteller auf, den Anforderungen der IT-Sicherheit besser nachzukommen.

Große Projekte, die eine ebenenübergreifende Zusammenarbeit erfordern, sind derzeit die EU-Dienstleistungsrichtlinie und die einheitliche Behördenrufnummer 115, was sich am Ausstellungsprogramm von Verwaltungen und Unternehmen sowie Vorträgen zeigte. Erstmals gab es in diesem Jahr zwei Foren, eins für Projekte aus Bund und Ländern im Public-Sector-Forum, ein anderes für Kommunen.

Behördenrufnummer im Herbst

Für die einheitliche Behördenrufnummer 115 wurde das Portal www.d115.de auf der Cebit freigeschaltet. Zurzeit arbeitet man an einem Feinkonzept und will im Herbst 2008 mit dem Pilotbetrieb in vier Regionen starten – ein Vorhaben, das im Unterschied zu anderen internationalen Beispielen wie „Call 311“ in New York, „101 England“ oder „3939 Service Public France“ drei Verwaltungsebenen verknüpft, die fortan zusammenarbeiten müssen.

Auf dem Messestand der Bundesverwaltung sah man unter dem Motto „Deutschland wird einfacher“ insgesamt 36 Projekte von acht Ausstellern – darunter der elektronische Personalausweis, die elektronische Steuererklärung Elster oder sogenannte Bürgerportale, die das Versenden und Empfangen von Nachrichten und Dokumenten im Internet zwischen Bürgern, Unternehmen und Behörden sicher und verbindlich gestalten sollen.

Um die umfassende Vernetzung der Stadt Friedrichshafen in vielen Bereichen geht es im Projekt T-City, (www.t-city.de), das Bürgermeister Josef Büchelmeier bei der Eröffnung des Public Sector Parc vorstellte. Für die Online-Bildungsplattform Edunex (Education Next Generation) von T-Systems fiel auf der Cebit der Startschuss. Edunex ermöglicht eine differenzierte Integration von Lerninhalten in den Unterricht. (ur)

RFID im Masseneinsatz: Regulierung in der Schwebe

Auch in diesem Jahr räumten die Cebit-Veranstalter dem Thema RFID mit dem „Forum AutoID/RFID“ und dem „AutoID/RFID Solutions Park“ viel Platz ein. Hersteller, Anwender und Interessengruppen stellten in Vorträgen und an Ständen die jüngsten Entwicklungen und Trends vor.

Nicht nur Neuentwicklungen wie Transponder auf Polymerbasis (PolyIC GmbH), günstigere Lesetore (Feig Electronic) und diverse Einsatzzwecke der Chips in Logistik, Automobil-, Luftfahrt- und Pharmaindustrie konnten Interessierte in den RFID-Arealen bestaunen. Dort wurde auch der kürzlich von der EU-Kommission vorgestellte Empfehlungsentwurf zu Datenschutz- und Sicherheitsaspekten beim Einsatz der Funkchips (ec.europa.eu/yourvoice/ipm/forms/dispatch?form=RFIDRec) diskutiert.

So reagierten die Branchenverbände AIM und Bitkom, die Standardisierungsorganisation GS1 Germany und das Informationsforum RFID mit einem Aufruf an die Politik, keine zusätzlichen gesetzlichen Regulierungen zu erlassen. Andrea Huber vom Informationsforum RFID betonte, dass viele Anreize für den Handel, RFID-Technologie im Endverbraucherbereich zu benutzen, wegfielen, würde es zu der im Entwurf vorgeschlagenen standardisierten Deaktivierung der Tags nach dem Kauf kommen. Dadurch entstünden zum Beispiel höhere Kosten durch die notwendige Ausstattung der Kassen, es gäbe Schwierigkeiten beim Löschen des Chips durch das Kill-Signal, und RFID-typische Zusatzanreize wie die beleglose Garantie fielen weg.

Gleichwohl sehen Hersteller wie IBM kein Problem in der standardisierten Deaktivierung. Alexander Gleick kommentierte das Kostenargument: „Wenn durch RFID im Endverbraucherbereich Personalkosten für Hunderte von Kassiererinnen eingespart werden können, sind die Kosten für zusätzliche Lesegeräte unerheblich.“ Noch bis zum 25. April können Interessierte den Entwurf kommentieren. *Susanne Schwonbeck*

Gedruckte RFID-Chips mit Polymer

Halbleiterstrukturen lassen sich auch mit Polymeren aufbauen. Dieses Prinzip nutzte die Fürther PolyIC GmbH (www.polyic.com) bei der Entwicklung eines RFID-Chips im HF-Bereich mit einem maximalen Speicher von derzeit 4 Bit. Das üblicherweise verwendete Silizium haben die Hersteller gegen ein Polymer und das Kupfer der Antenne gegen Aluminium ausgetauscht. Außerdem werden die Chips im Druckverfahren hergestellt, was die Kosten senkt. Bislang beträgt die Lebensdauer dieser Chips drei bis sechs Monate, was sich in Hinblick auf die Diskussion über die Deaktivierung von RFID-Tags vom Bug zum Feature entwickeln könnte. *S. Schwonbeck*

Weniger verlorenes Gepäck durch RFID-Tags

Siemens zeigte ein Beispiel für eine Förderanlage, die mit Barcode und RFID-Chips versehene Gepäckstücke transportiert. Das Transportsystem samt RFID-Tags und -lesestationen wird demnächst am Ausbau des internationalen Flughafens Wuhan, China, im Einsatz sein. Die mit dem IATA-Standard RP1740C konforme Anlage liest die verwendeten UHF-Transponder an insgesamt acht Stationen aus. Die Informationen werden an nahe den Lesegeräten befindlichen Computern verarbeitet. Laut Siemens soll das Zeit sparen. Ziel der Anlage ist es, die Anzahl fehlgeleiteter Gepäckstücke zu verringern und dadurch Kosten zu senken. *Susanne Schwonbeck*



KURZ NOTIERT

ERP aus Polen: Comarch, einer der größten polnischen Softwareanbieter, stellte sein neues ERP-System Altum vor. Die Software basiert auf Microsofts Visualstudio.net und SQL Server und richtet sich speziell an kleine und mittlere Handels- und Dienstleistungsunternehmen. Workflow- und Business-Intelligence-Tools, zum Beispiel zur Planungsumsetzung (Balanced Scorecards), gehören zum Lieferumfang.

Auf .Net-Pfaden: Seine neue Office Line nennt Sage „Evolution 2009“. Die ERP-Software, konzipiert für den Einsatz in Firmen mit zehn bis 200 Angestellten, arbeitet erstmals komplett auf .Net-Basis. Die Benutzerführung orientiert sich an Microsofts Office 2007. Mit dem neuen System lassen sich Rechnungen signieren und per E-Mail versenden. Für die notwendige Sicherheit garantiert der Signaturservice im Trust-Center der Deutschen Post.

SOA-Einstieg: Die ELO Digital Office GmbH wagt sich auf das Feld der Infrastrukturanbieter und zeigte erstmals ihren Business Logic Provider (BLP). Die Server-Komponente soll Applikationen SOA-getreu zu einem unternehmensübergreifenden Prozess verzahnen. Mithilfe diverser Tools sollen sich Unternehmensprozesse modellieren lassen.

Integration: Modus Consult aus Gütersloh will Microsofts Standardsoftware Dynamics Nav und das DMS/ECM-System ELO zusammenführen, und hat dazu die Komponente Archivelink entwickelt. Sie regelt die automatische, serverbasierte Ablage und Indizierung von Belegen sowie die Zuordnung von Dokumenten zu Stamm- und Prozessdaten in Dynamics-Nav. Bedient wird sie über die Standardsoftware.

Nvinity: Version 2.0 mit PPS-Modul

Das Stockacher Softwarehaus Nissen & Velten führte die Version 2.0 seiner .Net-Unternehmenssoftware Nvinity vor. Neu ist ein Modul zur Produktionsplanung und -steuerung (PPS) inklusive Produktionsleitstand. Eine Plantafel visualisiert die Auslastung der Ressourcen im Zeitverlauf. Hier lassen sich auch Produktions- und Betriebsaufträge sowie Arbeitsgänge planen. Der Benutzer kann Produktions- und Betriebsaufträge zwischenzeitlich „parken“, wenn Aufträge mit höherer Priorität vorgezogen werden müssen. Mit dem Angebot für Einzel-, Kleinserien- und Serienfertiger will Nissen & Velten neue Märkte erschließen. Ebenfalls neu sind die Module Anlagenbuchhaltung und Management-Informationssystem.

Oxaion steuert erstmals auf Prozesskurs

Ihre in Java entwickelte ERP-Suite hat die Oxaion AG um eine Business-Process-Management-Suite (BPM) ergänzt. Die Process Engine läuft im Anwendungsserver von Oxaion open und greift direkt auf die Geschäftsobjekte in der ERP-Software zu. Geschäftsprozesse und Workflows erstellt der Planer mithilfe eines grafischen Editors. Für Konfiguration und Customizing der Software musste man bislang den Programmcode über Tabelleneinstellungen ändern. Das soll nun über das Anpassen des Prozessmodells zu erledigen sein. Als BPM-Entwicklungsumgebung nutzt Oxaion die Eclipse-Plattform einschließlich des EMF (Eclipse Modeling Framework) sowie UML 2.0. Prozessbeschreibungen legt das BPM-System im XMI-Format (XML Metadata Interchange) ab.

Wilken wirbt mit leichter Bedienbarkeit

Der Ulmer Softwarehersteller Wilken brachte seine ERP-Suite 2008 mit nach Hannover. Die bereits in einer Vorversion präsentierte Oberfläche hat man überarbeitet, um den Mandantenwechsel sowie die Navigation über individuell definierbare Workflows zu vereinfachen. Ebenfalls mit Ajax-Antlitz zeigt sich die E-Business-Lösung Openshop 4.0. Die ERP-Suite hält sich bereits jetzt an die gesetzlichen Anforderungen zum einheitlichen europäischen Zahlungsverkehr (SEPA) und kann mit den Compliance-Richtlinien nach dem Sarbanes-Oxley Act (SOX) sowie mit der zur Terrorismusbekämpfung vorgeschriebenen Geschäftspartnerprüfung umgehen. Amüsant wirkte in diesem Kontext das Standmotto „Demonstration einer bedienungsfreundlichen Software“. Eine der ausgestellten Figuren im Straßenkämpfer-Look trug die gelbe Sonne der Anti-AKW-Bewegung mit dem leicht abgewandeltem Spruch „SAP nein danke“ auf ihrem Schild.

Lebenselixier für Mainframe-Anwendungen

Ein Werkzeugbündel namens Webmethods Application Modernization Suite zum Aufpolieren von Mainframe-Anwendungen hat die Software AG geschnürt. Die Tools sollen Altanwendungen in eine SOA-Welt hieven. Es gibt drei Varianten: Die Web Edition dient der Webanbindung ohne Eingriff in bestehende Anwendungen. Sie versieht die „Green-Screen“-Programme lediglich mit Weboberflächen. Die SQL Edition basiert auf den neuen Connex-Adaptern und bietet eine einheitliche Sicht auf relationale und nicht-relationale Datenquellen.

Die SOA-Ausgabe legt das Fundament für den serviceorientierten Betrieb und stellt die benötigten Werkzeuge: Applinx (Programmdialoge), Entirex (Entwicklung), Webmethods ESB (Ablauf von Services und Orchestrierung) sowie Centrasite (Service Governance und Lifecycle Management). Entirex 8.0 unterstützt lange Nachrichten unter dem Transaktionssystem CICS sowie asynchrone und gesicherte Serviceaufrufe. Entwickler sollen so ohne Änderungen Programmcode zu .Net-, J2EE- oder Webservices kapseln können.

Um die Zerlegung von Altanwendungen in Services zusätzlich zu fördern, schloss die Software AG ein Wiederverkäuferabkommen mit Relativity Technologies. Deren Modernization Workbench bietet optional die automatisierte Analyse, Dokumentation und das Refactoring von alten Programmen.

Varial mit Controlling-Werkzeug

Die Siegener Varial Software AG, eine Tochter der Infor-Gruppe, ergänzt ihre Finanzmanagement-Software Varial World Edition um eine Controlling-Komponente, den Varial Planner. Über ihn stoßen die Benutzer Analyse- und Planungsprozesse an. Das Werkzeug ist in drei Versionen erhältlich. Für den Einstieg eignet sich die Smart Edition, mit der sich aus der Gewinn- und Verlustrechnung ein Kennzahlensystem erstellen lässt. Zusätzliche Funktionen für Simulationen und tiefergehende Analysen bietet die Business Edition. Die Enterprise Edition umfasst acht Planungsebenen, beispielsweise auf der Basis von Budget, Prognosen, Best-, Worst- oder Real-Cases. Zudem erlaubt das Tool einen von der einzelnen Kostenstelle nach oben verlaufenden Planungsprozess. Ein rückblickender Vergleich kann eine Zeitspanne von bis zu fünf Jahren umfassen.



Nürnberger Messe auf Wachstumskurs

Alles drin

Axel Urbanski, Jürgen Seeger, Nikolai Zotow

Ein passendes Bett hat sich die Embedded World in Nürnberg bereitet. Die Messe ist mittlerweile das weltweit größte Ereignis in diesem Marktsegment.

Auf circa 30 000 Quadratmetern in vier Hallen stellten Ende Februar 675 Aussteller aus über 60 Ländern ihre Lösungen und Produkte aus den Bereichen Hardware, Tools, Anwendungssoftware und Dienstleistungen vor.

Neben der eigentlichen Ausstellung thematisierte ein Kongress die aktuellen Themen dieses Marktsegments, unter anderem Multi-Core-Systeme, Lösungen im Automobilbau, TCA, Digital Signal Processing und Fragen der Architektur im Embedded-Bereich.

Intel präsentierte im Rahmen einer Pressekonferenz neue Prozessoren für den Embedded-Markt auf Basis der 45-nm-Fertigungstechnologie. Die neuen Xeon-5400-Quad-Core- und Xeon-5200-Dual-Core-Prozessoren eignen sich laut Hersteller in Verbindung mit dem 5100 Memory Controller Hub (MCH) für wärmeempfindliche Blade-Umgebungen wie den Einsatz in Speicherlösungen, Routern oder medizinischen Geräten.



Wachsende Bedeutung von Embedded Software: Keynote-Redner Bharat Balasubramanian (Daimler AG)

Sparsamer und schneller

Laut Hersteller verringert die eingesetzte HKMG-Halbleitertechnik (High-k Metal Gate) nicht nur den Stromverbrauch, sondern steigert auch die Schaltgeschwindigkeit. Der Life-Cycle-Support für die neuen Prozessoren wurde von fünf auf sieben Jahre verlängert – ein klares Signal in Richtung verlässliche Liefersituation. Intel-Konkurrent AMD gibt eine Zeitspanne von fünf Jahren an, die individuell vertraglich verlängert werden kann.

Mit dem ADP1043 geht Analog Devices im Bereich der Stromversorgung neue Wege. Der Netzteilsteuerchip verfügt über eine I^2C-Schnittstelle (Inter IC Bus) zur Steuerung des Chips, was den Entwurf intelligenter Netzteile erheblich erleichtern soll. Die wichtigen Eigenschaften der Stromversorgung lassen sich via Software einstellen und überwachen.

Texas Instruments (TI) gab erste Informationen über die mit der neuen „Multi-Core“-Application-Prozessorfamilie OMAP35x verfolgte Strategie. Es handelt sich dabei nicht um klassische Multi-Core-CPUs, sondern um die Vereinigung verschiedener Rechenkerne auf einem Chip. Gemeinsam ist allen ein ARM-Cortex-A8-Kern. Die Familie wird mit der Zeit auf vier pin- und softwarekompatible Bausteine wachsen. Die einzelnen Mitglieder unterscheiden sich durch die Zusammenstellung der weiteren Kerne. Es soll mindestens noch einen DSP und einen 2D-/3D-Grafikkern geben.

Wind River, unter anderem bekannt für hardwarenahe und integrierte Entwicklungsumgebungen, zeigte seine Erweiterung für die neuesten Prozessoren. Die Wind River Workbench erlaubt das On-Chip-Debugging über die JTAG-Schnittstelle. Voraussetzung ist eine JTAG-Box wie Wind River ICE. Für die linuxbasierte Mobilfunkplattform Android waren verschiedene Anpassungen an Prozessoren wie OMAP3430 von TI, Nomadik-CPUs von STMicroelectronics sowie NECs Medity M2 zu sehen.

Der Fraunhofer Verbund für Informations- und Kommunikationstechnik präsentierte Systeme im Automobilbereich wie die Initiative AUTOSAR. Dabei handelt es sich um eine Spezifikation für die Laufzeitumgebung von Software in Fahrzeugen. Das Fraunhofer-Institut für Integrierte Schaltungen stellte seine Sensornetztechnik am Beispiel der Fernablesung von Gaszählern vor. In Zusammenarbeit mit der österreichischen Firma Veraut werden Haushaltszähler mit preisgünstigen Funkknoten statt teuren GSM-Modulen ausgestattet, die ihre Daten an einen Masterknoten übermitteln. Von dort werden sie wiederum über Powerline Communication an einen Zentralserver übersandt.

Modellierung via UML gefragt

Bei Frauenhofer FOKUS ging es darum, neue Fahrzeugfunktionen in einem Fahrsimulator zu erproben. Als Werkzeuge kommen modellbasierte Tools zum Einsatz, die auf Basis der Unified Modeling Language arbeiten. UML respektive Modellierung und andere „moderne“ Ansätze der Softwareentwicklung stießen überhaupt auf großes Interesse in Nürnberg. So war ein einführender UML-Vortrag eines Willert-Consultants übervoll, und an vielen Ständen war zu hören, dass man eine schnellere Adaption der aus der Mainstream-IT bekannten Methoden erwarte. Bei Willert war auch das Embedded UML Studio auf Rhapsody-Basis zu sehen, mit UML-2.0- und SysML-Unterstützung.

Auf die Model Driven Architecture (MDA) und SOA setzt das Beratungshaus Itemis, das für sein Integrationsprojekt Yakindu von der Innovationsinitiative „Deutschland – Land der Ideen“ ausgezeichnet wurde. Yakindu soll den Entwicklern von Embedded Software Werkzeuge an die Hand geben, mit denen sie schneller und besser programmieren und testen können. Im Mittelpunkt stehen möglichst genaue digitale Modelle der zu entwickelnden Systeme, mit deren Hilfe Teile der Software automatisch erzeugt, ihre Wirkung simuliert und das Zusammenspiel mit den anderen Komponenten geprüft werden kann.

Artisan Studio ist ein weiteres Modellierungswerkzeug für komplexe technische Systeme, unterstützt UML 2.0 und SysML sowie die Programmiersprachen Ada, C, C++, C# und Java. Es läuft auf Windows als Single- oder Multi-user-Client, inklusive Support für Microsofts und Citrix’ Terminal Server.

Den Lebenszyklus im Blick

Anderes Hype-Thema in der Softwareentwicklung derzeit: Application Lifecycle Management. Polarion zeigte sein Tool ALM for Subversion, das auf Grundlage der freien Versionsverwaltungssoftware eine Planung des gesamten Prozesses vom Design über das Testen bis zur Wartung ermöglicht. MKS fokussierte seinen Auftritt auf Application Lifecycle Management, das Softwarepaket Integrity soll ein nahtloses Zusammenspiel von Requirements-, Test-, Release-, Konfigurations- und Change-Management ermöglichen. Die ITIL-zertifizierte Suite ist multiplattformfähig und ermöglich die Integration in Help-Desk-Umgebungen. Auffällig oft tauchten im Zusammenhang

mit Softwareentwicklung die Begriffe Qualitätssicherung und Testen auf.

Pars pro toto genannt seien etwa Vectorcast und die Tools der Oldenburger Embedded Systems AG. Ersteres ist ein von QA Systems vertriebenes Tool zum automatischen Testen von C- und C++-Programmen. Neben Unit- und Integrations-Tests unterstützt es unter anderem Code-Abdeckungsanalysen und benutzerdefinierte Tests der Erfüllung von Anforderungen (www.vectorcast.com). Die Oldenburger sind mit zwei Werkzeugen im Umfeld modellbasierten Testens aktiv: Embedded Validator und Targetlink Model Checker, mit denen beispielsweise ein automatischer Robustheitstest möglich ist.

Auch der universitäre Bereich war in Nürnberg vertreten. Über Benchmark-Ansätze und -algorithmen informierte die Hochschule Harz, die Technische Universität Ilmenau zeigte zwei Projekte. Eins beschäftigt sich mit frühen Entwicklungsphasen im Systementwurf, das andere mit verteilten eingebetteten Systemen im Automobilbereich. Die Schweizer Hochschulen waren mit einem Gemeinschaftsstand präsent. Unter anderem bot dort die Fachhochschule Nordwestschweiz die Portierung von Linux auf spezielle Hardwareplattformen inklusive Entwicklungen von Gerätetreibern an.

Im boomenden Marktsegment

Die Embedded World hat sich auch dieses Mal gegenüber dem Vorjahr erweitert. Waren im Jahr 2007 noch 590 Unternehmen auf der Messe präsent, haben sich dieses Jahr schon 670 Aussteller für einen Messeauftritt entschieden, davon 40 % aus dem Ausland. Laut Veranstalter vergrößerte sich die Ausstellungsfläche um 18 %. Die nächste Embedded World findet vom 3. bis 5. März 2009 in Nürnberg statt. (JS)

Bitkom verstärkt Embedded-Systems-Aktivitäten

Anlässlich der Embedded World gab der ITK-Branchenverband Bitkom bekannt, seine Aktivitäten zu Embedded Software ausbauen zu wollen. So hat der Ende 2007 gegründete Arbeitskreis „Softwareintensive eingebettete Systeme“ eine Studie in Auftrag gegeben und will „Embedded Software für Öffentlichkeit und Politik als eigenständigen Wirtschaftsfaktor greifbar machen.“

Denn die im Auftrag des Bitkom von Roland Berger erstellte Studie „Die Zukunft der Digitalen Wirtschaft“ nennt Embedded Systems als eines von sechs strategischen ITK-Wachstumsfeldern. Das weltweite Marktvolumen wird dort auf 138 Milliarden Euro geschätzt, das jährliche Wachstum bis 2010 auf neun Prozent. In umsatzstarken vertikalen Märkten seien Embedded Systems der entscheidende Treiber von Produktinnovationen. So sind laut Studie rund 90 Prozent aller Innovationen im Automobilsektor ITK-basiert.

Die Berger-Studie sieht zwar Deutschland durch seine solide industrielle Basis in einer traditionell starken Position. Doch der Wettbewerbsdruck steige, unter anderem bedingt durch die intensive staatliche Förderung besonders in den asiatischen Ländern.

Dennoch existieren in Deutschland bislang kaum Marktdaten zu diesem bedeutenden Querschnittssegment. Der Bitkom hat darum Pierre Audoin Consultants (PAC) und Techconsult mit einer Studie beauftragt, deren Ergebnisse im Herbst präsentiert werden sollen. Die Erhebung soll die bisher auf vertikale Märkte fokussierten Daten ergänzen, das Gesamtmarktvolumen ermitteln sowie die Auswahl zukünftiger nationaler Förderschwerpunkte und die Bildung regionaler Cluster unterstützen. Den Fragenkatalog haben die Bundesministerien für Bildung und Forschung (BMBF) sowie für Wirtschaft und Technologie (BMWi) mitentwickelt.

iX-Veranstaltungen

www.ix-konferenz.de.

Gleich drei neue Veranstaltungen können wir dieses Mal ankündigen. Der Reihe nach:

– Die erfolgreichen zweitägigen Workshops zum Thema **Computer-Forensik** mit Alexander Geschonneck, dem deutschen Forensik-Spezialisten, als Referent finden auch in diesem Jahr statt, und zwar im Juni in Berlin und München. Die Veranstaltung bietet Sicherheitsbeauftragten, Administratoren, Beratern und IT-Revisoren die Möglichkeit, sich in Theorie und Praxis der digitalen Spurensuche einzuarbeiten.

– Mit der **Windows PowerShell** hat Microsoft die Macht der Kommandozeile entdeckt. Allerdings ist deren Nutzung nicht ganz trivial, sprich: Man tut gut daran, sich ein bisschen einzuarbeiten; etwa durch den Besuch eines der dreitägigen PowerShell-Seminare, die unser langjähriger Autor Holger Schwichtenberg im April, Juni und Oktober in Essen anbietet. Koreferent ist Peter Monadjemi, auch nicht gerade ein Unbekannter im Windows-Umfeld.

– Im Juni sollten mindestens diejenigen einen Tag freischaufeln, denen der Ausdruck „die drei Amigos“ etwas sagt. Damit gemeint sind die UML-Erfinder Grady Booch, James Rumbaugh und **Ivar Jabobson**. Letzterer führt in die Ganz-weit-vorne-Trends der Softwareentwicklung ein. Unter dem bescheidenen Titel „Back to Basics“ geht es um „Getting Good Software Quickly and at Low Cost“. Frankfurter, Hamburger, Münchner und Stuttgarter müssen nicht einmal das Reisekostenbudget belasten.

Wer an diesen vier Juni-Terminen absolut nicht kann, schafft es vielleicht zur **Teamconf 2008**, der Konferenz zu Microsofts Visual Studio Team System vom 22. bis 24. April in München. Dort tritt Ivar Jacobson nämlich als Keynote-Redner auf.

Und: Wie angekündigt, haben wir noch zwei weitere **Kerberos-Workshops** organisiert, im April und Juni in Düsseldorf respektive München, da die ersten drei Termine ausgebucht waren.

Details zu allen Veranstaltungen sind wie gewohnt auf der Konferenz-Website www.ix-konferenz.de zu finden.



Zwei der bekanntesten Autoren zu Windows-Themen in Deutschland: Holger Schwichtenberg (links) und Peter Monadjemi (rechts) vermitteln ihr Wissen über die PowerShell.

Heise-Security-Konferenz: Was die sichere Firmen-Website kostet

Die diesjährige Heise-Security-Konferenz „Die sichere Firmen-Website“ legt den Schwerpunkt auf die Kosten-Nutzen-Analyse von Sicherheitsinvestitionen. Dazu analysieren ausgewählte Experten unterschiedliche Bedrohungsszenarien, präsentieren mittel- und langfristige Strategien zur Erhöhung der Sicherheit und geben einen Überblick über die gängigen Tools und Produkte. Ein separater Vortrag beschäftigt sich mit der Auswahl des richtigen Bezahlsystems. Der für die Onlinesicherheit der größten Schweizer Bank Zuständige gewährt Einblicke in seinen Erfahrungsschatz. Und der Justiziar des Heise-Verlags sorgt für mehr Rechtssicherheit im Dschungel von Haftungsrisiken und Hackerparagrafen.

Die eintägige Veranstaltung findet am 17. April in Karlsruhe, am 24. April in Düsseldorf, am 29. April in München und am 6. Mai in Hamburg statt. Weitere Details und Anmeldeinformationen finden sich auf den Konferenzseiten von Heise Events: www.heise.de/events/2008/heisec_konferenz/

Open Source in Embedded Systems

Der Messeauftritt des Open Source Automation Development Lab (OSADL, www.osadl.org) zeigte auch in diesem Jahr die wachsende Bedeutung von Open Source im Embedded-Systems-Umfeld. Die Ende 2005 gegründete Genossenschaft hat mittlerweile 21 Mitglieder, überwiegend im deutschsprachigen Raum. Kurz vor der Messe war der Darmstädter GUI-Spezialist Basyskom beigetreten, bekannt geworden unter anderem durch sein Open Palmtop Integrated Environment (OPIE).

Die Mitgliedsfirmen decken unterschiedliche Aspekte der Softwarenutzung in Embedded Systems ab. Der nächste OSADL-Messeauftritt ist im April auf der HMI im Application Park in Halle 17.

GUI im Gerät integriert

Die österreichische Firma Ajaxup zeigte ihre gleichnamige Lösung, die es ermöglicht, ein HTML-Javascript-GUI auf Micro-Devices unterzubringen. Dabei geht es vor allem auch um solche Systeme, die keinen Platz für einen TCP/IP-Stack haben. Als Beispiele zeigen die Entwickler einen Zigbee-Sensor mit 90 KByte Speicher und eine 70 KByte große Smartcard, die über die jeweils vorhandenen Kommunikationsprotokolle angesprochen werden können und daraufhin ihre Bedienoberfläche schicken. Details: www.ajaxup.com

.Net für Kleinstgeräte

Microsoft stellte auf seinem Stand eine neue Version des .Net Micro Framework für Kleinstgeräte vor. Es bietet Unterstützung für Web Services on Devices (WSD) und einen integrierten TCP/IP-Stack. Die Implementierung des Device Profile for Web Service ist nun mit der in Vista und anderen Produkten aus Redmond kompatibel.
Das WSD ermöglicht den Austausch von Geräteinformationen, die nötig sind, um eigene Ressourcen im Netz bereitzustellen. Außerdem zeigte der Softwarehersteller eine in Zusammenarbeit mit IBM erstellte Point-of-Service-Lösung für den Einzelhandel und das Hotelgewerbe. Windows Embedded for Point of Service (WEPOS) wird zukünftig auf Big Blues Point-of-Sale-Systemen Anyplace Kiosk, Self-Checkout und SurePOS 700 zum Einsatz kommen.

Virtualisierung mit Lynxsecure

Version 2.0 von Lynxsecure stellte der kalifornische Anbieter Lynuxwork vor, einen „Separation Kernel und Embedded Hypervisor“. Lynxsecure 2.0 virtualisiert die zugrunde liegende Hardware, um sie mehreren Betriebssystemen parallel anbieten zu können. Dem Embedded Hypervisor fällt dabei die Aufgabe zu, die Koexistenz von Echtzeitbetriebssystemen wie dem hauseigenen RTOS mit „normalen“ Betriebssystemen wie Linux oder Windows herzustellen. Der Separation Kernel sorgt für die Aufteilung der Ressourcen sowie eventuellen Datenaustausch zwischen den verschiedenen Partitionen.

LynxSecure 2.0 soll ab Sommer 2008 erhältlich sein und läuft laut Hersteller auf allen 32- und 64-Bit-CPUs mit MMU.

Patientenabrechnung mit Linux

Der Kartenleser „Medcompact“ von Thales-e-Transactions, der ab Mitte Juli 2008 in Deutschland verfügbar sein soll, läuft unter der Embedded-Linux-Distribution ELinOS des Herstellers Sysgo. Der in der Patientenabrechnung einsetzbare Kartenleser verfügt über Open SSH für die Datenverschlüsselung und soll nach dem Signaturgesetz von der Bundesnetzagentur EAL 3+ zertifiziert werden.

VMworld Europe 2008

Über den Teich

Jörg Riether

Automatisches Desaster Recovery, überwachte Gastsysteme und Portabilität bildeten die thematischen Highlights der ersten VMworld Europe.

Erstmals fand die VMworld, Hausmesse VMwares und größte Virtualisierungskonferenz, den Weg über den Atlantik nach Europa. Über 4500 Teilnehmer kamen Ende Februar nach Cannes, um sich im Palais des Festivals über die aktuellen Virtualisierungstrends zu informieren. Und die gehen gebündelt in eine Richtung: Sicherheit in all ihren Facetten. Angefangen bei Desaster-Recovery-Szenarien bis hin zur Sicherheit der Gastsysteme.

Das war noch zu Beginn der Konferenz nicht zu erwarten: VMwares CEO Diane Greene richtete ihre Keynote vor allem am momentanen Hype Desktop-Virtualisierung aus. Dazu zeigte sie in einer Live-Demo, wie man einen virtuellen Desktop etwa vor einer Reise einfach auf die lokale Festplatte seines Notebooks „aus-checken" kann. Die Software schreibt eine Art Replikat auf die Festplatte, und danach kann man diese virtuelle Maschine (VM) einfach mitnehmen und lokal starten. Der Clou: Kommt man später wieder zurück und hat Zugriff auf das Host-System, oder hat man unterwegs etwa über VPN Zugriff auf das LAN, kann man seine veränderte Version einfach mit dem Host synchronisieren. Ein smarter Seitenhieb in Richtung Microsoft durfte natürlich nicht fehlen: „I think the most time-consuming part of this demo is booting Windows."

Abschließend präsentierte sie als kleines Schmankerl ein Projekt aus dem jüngsten Zukauf Thinstall. Auf einem Rechner, der kein Microsoft Visio installiert hatte, startete sie Visio in einer einzigen Datei von einem USB-Stick. Intern führt VMware Thinstall als Beta unter dem Codenamen „Project North Star" und gab es noch am ersten Konferenztag zum Download für interessierte Beta-Tester unter www.vmware.com/beta/northstar frei. An dieser Stelle sei noch auf eine echte Besonderheit hingewiesen: Ein Thinstall-Programm ist eine einzelne *.exe*-Datei, die man von einem beliebigen Ort aus starten kann, auch ohne jegliche Adminrechte.

Servicepakete zum Herunterladen

VMwares Chef-Vordenker Mendel Rosenblum, der mit seiner Rede den zweiten Konferenztag eröffnete, stellte gleich zwei neue Techniken vor: vServices und VMsafe. Hinter vServices verbirgt sich ein neuer Ansatz von Virtual Appliances. Verstand man bislang darunter eine einzelne virtuelle Maschine, die man aus dem VMTN (VMware Technology Network) herunterladen konnte, geht man bei VMware einen Schritt weiter: Demnächst kann man ganze Services herunterladen, auch wenn ein einzelner zum Beispiel aus mehreren VMs besteht. Sie alle sind in einem einzigen Paket gebündelt und lassen sich komplett als solches starten. Außerdem kommen die vServices im Open Virtualization Format (OVF) und haben Metadaten an Bord, die Details wie virtuelle Ressourcenzuweisungen enthalten.

VMsafe hingegen realisiert ein neues Sicherheitskonzept. Man darf sich unter VMsafe ein Set aus diversen APIs vorstellen, die Zugriffe von außerhalb der virtuellen Maschine auf den jeweiligen Speicher, die CPU, die Festplatte und die Netzwerkkarte der VM gestatten und zwar laut Rosenblum in Echtzeit auf „jedes einzelne Byte". In der zugehörigen Live-Demonstration war eine solche Protection Engine zu sehen, die den Hauptspeicher einer VM als Memory Map live grafisch darstellte. Sie erkannte eine eingeschleuste Malware von außen auf Hypervisor-Level und stoppte sie, bevor ein Benutzer sie in der eigentlichen virtuellen Maschine ausführen konnte. Rosenblum betonte, dass VMware in dieser Richtung bereits mit Sicherheitsunternehmen wie McAfee, Checkpoint, Symantec, Trend und Sophos eng zusammenarbeitet.

Zur Idee der Continuous Availability, einer echten Replikation aller Änderungen innerhalb einer VM auf ein zweites Live-System, gab Rosenblum keine weiteren Details bekannt. Er hatte sie erstmals auf der VMworld 2007 in San Francisco vorgestellt, wo sie viel Beachtung fand. Darauf darf man auch weiterhin gespannt sein, würde es doch die Desaster Recovery grundsätzlich neu definieren.

Eher im Stillen stellte VMware ein echtes Highlight vor: Der Site Recovery Manager, ein neuartiges Automatisierungstool für Desaster-Recovery-Szenarien im SAN (Storage Area Network), erregte einiges Aufsehen. Zwar will das Softwarehaus die erste Release voraussichtlich erst im Mai freigegeben, dennoch konnte man sich am Dell-Equallogic-Stand einen umfassenden Eindruck davon verschaffen. Der Site Recovery Manager soll die komplette Desaster-Failover-Interaktionen zwischen Virtual Center und dem jeweiligen SAN komplett automatisieren – sowohl als Simulationslauf als auch im Ernstfall. Darunter fallen etwa die Unterbrechung der aktiven Replikation, die Hochstufung des Replikats zum Master und ihre produktive Übernahme.

Voraussetzung dafür ist eine Unterstützung der entsprechenden Speicher-Subsysteme durch VMware, da der Site Recovery Manager in der Lage sein muss, entsprechende Instruktionen an sie zu senden und von ihnen zu empfangen. Bei Dell-Equallogic sah das Ganze bereits jetzt recht ausgereift aus: In der Vorführung konnte er mehrere virtuelle Maschinen, die einem simulierten Subsystem-Crash zum Opfer fielen, automatisch wiederherstellen.

Im Ausstellungsbereich der Konferenz tummelten sich unter den zahlreichen Anbietern auch die direkten Konkurrenten Citrix, Microsoft und Parallels, die alle drei als Gold-Sponsoren auftraten. Parallels hat zurzeit den Parallels Server, Microsoft sein Hyper-V in der Mache, das sich momentan im Beta-Stadium befindet. Beide Produkte sind für Mitte des Jahres zu erwarten.

Die Serverhersteller Dell, HP, IBM und Fujitsu-Siemens kündigten währenddessen Servermodelle mit vorinstalliertem ESX 3i Hypervisor an, von denen inzwischen das eine oder andere verfügbar sein sollte.

Insgesamt nahmen die Besucher die erste Auflage der europäischen VMworld überaus positiv auf. Sie dürfte sich bereits zum jetzigen Zeitpunkt als fester Bestandteil der VMworld-Konferenzen etabliert haben. Nächster Termin im VMworld-Kalender ist der September. Dann öffnet die VMworld 2008 in Las Vegas ihre Tore. Dort darf man dann auf mehr Details zum Thema Continuous Availability hoffen. (sun)



Der Meister in seinem Element: Chef-Vordenker Mendel Rosenblum stellt die jüngsten VMware-Entwicklungen vor.

10. Deutscher Perl-Workshop ohne Perl 6

Kein Ende in Sicht

Christian Kirsch

Auch nach zehn Jahren hat der Deutsche Perl-Workshop nichts von seinem Charme verloren. Auf Neuigkeiten von Perl 6 wartete man zwar vergeblich, dafür gab es jedoch tiefe Einblicke in die aktuellen Möglichkeiten der Skriptsprache.

Von vielen anderen Veranstaltungen unterscheidet den Deutschen Perl-Workshop, dass ihn Privatleute in ihrer Freizeit organisieren. Das hält die Kosten konkurrenzlos niedrig und schafft eine familiäre Atmosphäre. Zu erfahren war dies erneut bei der Ende Februar zum zehnten Mal stattfindenden Auflage der Veranstaltung.

Zwar fehlten diesmal die internationalen Perl-Stars, immerhin war in der Vergangenheit Damian Conway zweimal zu Vorträgen angereist. Ausgleich schafften jedoch einheimische Größen, von denen unter anderem Andreas König und Marc Lehmann bereits beim ersten Workshop vorgetragen hatten. König beschrieb diesmal den aktuellen Stand der öffentlichen Modul-Tests und forderte die Teilnehmer auf, sich daran zu beteiligen, denn nur durch zahlreiche Tester lasse sich die Qualität der Perl-Module gewährleisten.

Best Practices im Doppelpack

Maximilian Maischein steuerte ein Tutorial zur Perl-Programmierung für Fortgeschrittene bei sowie einen Vortrag über *Web::Scraper*, das über sein eigenes Modul *Web::Mechanize* hinausgehende Fähigkeiten zum automatischen Auswerten von Webseiten bietet. Steffen Winkler und Renee Bäcker befassten sich mit Damian Conways Buch „Perl Best Practices“. Ersterer hatte einen Beitrag zu seinen Erfahrungen damit angekündigt, beschränkte sich jedoch auf ein langatmiges Referieren von Conways Vorschlägen. Bäcker stellte *Perl::Critic* vor, mit dem sich Kodierungsrichtlinien kontrollieren lassen. Dieses Modul verwendet sogenannte Policy-Dateien, von denen die meisten auf „Perl Best Practices“ beruhen.

Nur mittelbar mit Perl hatte Tina Müllers Beitrag über Cross-Site Scripting und Cross-Site Request Forgery zu tun. Sie präsentierte ein Verfahren, mit dem Script-Autoren den Missbrauch ihrer Webseiten durch Angreifer verhindern können. Es beruht im Wesentlichen auf unsichtbaren Feldern in Webformularen, deren benutzerabhängigen Inhalt die Website regelmäßig modifiziert.

Dass Perl trotz des zunehmenden Einsatzes von Ruby, Python und PHP immer noch im Unternehmensumfeld eine wichtige Rolle spielt, illustrierten die Beiträge von Stefan Hornburg zu Request-Trackern und von Wolfgang Kinkeldei über die Druckvorlagenherstellung mit Perl und Applescript. Das von ihm vorgestellte Verfahren kommt beim Produzieren von Etiketten für Sportschuhe zum Einsatz.

Ganz und gar ruhig blieb es um das Thema „Perl 6“; weder zu Parrot noch zu Pugs gab es Vorträge. Auch Jonathan Worthingtons „Parallel New World“ befasste sich nur mit möglichen Parallelisierungstechniken, die unter Umständen in die nächste Version der Sprache einziehen könnten. In Gesprächen war immer wieder Skepsis zu spüren, ob es jemals ein Perl 6 geben werde. Die Arbeit daran dauert nun schon seit 2000 an.

Im nächsten Jahr soll der Deutsche Perl-Workshop in Frankfurt/Main stattfinden, organisiert von der dortigen Perl-Mongers-Gruppe. (ck)

Tangible and Embedded Interaction in Bonn

Touch me

Christian Geiger

Drahtlose Netzwerke, günstig verfügbare Sensoren und die Miniaturisierung leistungsfähiger Recheneinheiten haben in den letzten Jahren einen neuen Schwerpunkt in der Mensch-Maschine-Kommunikation ermöglicht.

„Tangible and Embedded Interaction (TEI)“ heißt das Gebiet, in dem Forscher weltweit daran arbeiten, die Interaktion mit Anwendungen (be-)greifbar zu machen. Auf der diesjährigen TEI-Konferenz – vom 18. bis 20. Februar – konnten 150 Wissenschaftler aus der ganzen Welt ihre Erkenntnisse austauschen.

„Informationen unauffällig an nützlichen Orten und zu angebrachten Zeiten einzubetten, ohne dass vom Benutzer ein ausdrücklicher Befehl erwartet wird“ ist für Professor Albrecht Schmidt von der Universität Duisburg-Essen eines der Ziele. Er verdeutlichte dies am Beispiel einer High-Tech Visitenkarte: Legt man sie aufs Telefon, initiiert sie einen Anruf, hält man sie an einen Bilderrahmen, werden Bilder der Person angezeigt und nähert sie sich schließlich einem Webbrowser, wird die Homepage der Person geöffnet.

Ein Schwerpunkt der vorgestellten Projekte war die Musikerzeugung. Die belgische Firma Percussa präsentierte ihr Produkt Audiocubes. Dabei benutzt man handgroße transparente Würfel zur Audiosynthese, die durch LEDs im Innern unterschiedliche Farben annehmen können. Die Würfel sind mit Ein- und Ausgängen für Audio ausgestattet und besitzen an jeder Seite einen Infrarotsensor, der andere Würfel in der Umgebung entdecken kann. Je nachdem, welche Würfelseiten in welchem Abstand zueinander stehen, lassen sich Töne erzeugen, Effekte modulieren oder über einen angeschlossenen Rechner Synthesizeranwendungen steuern. Da jeder Würfel einen eigenen digitalen Signalprozessor besitzt, ist eine Musikerzeugung ohne angeschlossenen Rechner möglich.

Ein ähnliches Interaktionskonzept verfolgt das Projekt Xenakis der Uni Augsburg, das als innovativste Idee auf der Konferenz ausgezeichnet wurde. Verschieden geformten Spielsteinen sind bestimmte Instrumente, Tonhöhen und Tonlängen zugeordnet. Legt man die mit Markierungen an der Unterseite versehenen Objekte auf eine Glasplatte, erkennt eine darunter montierte Kamera die Position und wandelt diese in Toneffekte um. Die Entfernung der Steine zueinander bestimmt, welches Instrument welchen Ton mit welcher Dauer spielt. Bei mehreren Möglichkeiten entscheidet ein Zufallsalgorithmus in Abhängigkeit von der Entfernung zwischen den Objekten.

Steffi Beckhaus von der Universität Hamburg bot mit ihrem „Granulatsynthese“-Projekt ein besonderes audio-haptisches Erlebnis. Bewegt der Benutzer seine Hände in einer Menge von Vinylgranulat auf einem Glastisch, wird dies durch eine Kamera unter dem Tisch erkannt. Das Auftürmen von Bergen oder Aushöhlen von kleinen Mulden verändert die Transparenz der Substratmenge und erzeugt einen veränderlichen Klangteppich meditativen Sounds (s. Abbildung).

Man spürt förmlich das Erzeugen der Töne mit den Händen. Noch einen Schritt weiter geht das Projekt „DrawSound“ des Japaners Kazuhiro Jo von der Universität Tokio. Er verfolgt die Pinselführung beim Malen und bildet Länge, Dicke oder Schwung des Pinselstrichs auf Audioparameter ab. Je nach Mapping ertönen höhere und leisere Töne, je mehr am oberen linken Bildrand gemalt wird. Ein klassisches Musikstück wird schneller gespielt, je schneller sich der Pinsel über die Leinwand bewegt – man malt praktisch die Musik.

Eine kurze Zusammenfassung aller Projekte, viele Fotos und weitere Informationen zu dieser spannenden und gut organisierten Konferenz findet man unter www.tei-conf.org. Im nächsten Jahr treffen sich die User-Interface-Spezialisten im englischen Cambridge. (WM)



Klänge mit den Händen formen: das Granulatsynthese-Projekt der Universität Hamburg



Mobile World Congress in Barcelona

Das Netz rückt näher

Kay Glahn

Nachdem der 3GSM World Congress vor zwei Jahren von Cannes nach Barcelona umgezogen ist, hat er nun seinen Namen geändert und firmiert als Mobile World Congress. Branchengrößen wie Nokias Chef Olli-Pekka Kallasvuo sowie die CEOs von Cisco und Vodafone beschrieben den aktuellen mobilen Markt.

Wichtiges Thema des Mobile World Congress war neben mobilen Diensten und Übertragungsverfahren der nächsten Generation vor allem der Wettbewerb zwischen den großen Netzbetreibern und Geräteherstellern. Zahlreiche Dienste und wachsende Bandbreite wiesen darauf hin, dass das mobile Internet nun Realität wird. Außerdem setzen sich anscheinend GPS-Empfänger in Mobiltelefonen durch. Hersteller wie Nokia, Toshiba, HTC und Samsung haben solche Geräte vorgestellt, und einige bieten dazu passende Dienste an. Der Navigationsgerätehersteller Garmin stellte mit dem Nüviphone ein Handy mit Touchscreen vor, das Telefonie, Internet und GPS in einem Gerät vereint und beispielsweise Google-Ergebnisse nach der Entfernung vom Standort ordnen kann.

Viele Firmen kündigten neue Dienste oder Partnerschaften an. T-Mobile will mit Yahoo und nicht mehr wie bisher mit Google zusammenarbeiten, und Nokia tut sich mit Google und Orange zusammen. Google liefert dabei die Basis für „Nokia Search“, das sowohl eine lokale als auch eine netzweite Suche bietet. Mit Orange will man bei ortsbezogenen Diensten, Karten, mobiler Werbung und Spielen zusammenarbeiten – alles Bereiche, in denen Nokia bereits mit seinem OVI-Service aktiv ist. Maps 2.0, die neue Version von Nokias Navigationslösung, hilft auch Fußgängern beim Zurechtfinden. Die Firma propagierte ihre serviceorientierte Philosophie, in der Ort und Zusammenhang eine wichtige Rolle spielen und sich Geräte der jeweiligen Situation anpassen.

Push-Mail für Heimanwender

Yahoo stellte mit One-Connect in Barcelona einen neuen Service für Mobiltelefone vor, der Inhalte verschiedener sozialer Netze und Messaging-Anbieter aggregiert und mit dem lokalen Adressbuch verknüpft. LogMeIn präsentierte eine Remote-Support-Lösung für Geräte mit Symbian S60, und RIM zeigte mit Unite-Server eine kostenlose Push-Mail-Variante für Blackberry-Geräte. Sie wendet sich an Privatkunden, die sie auf ihrem Heimrechner installieren können. Mit Vodafone zusammen plant RIM die Entwicklung von Blackberry-Diensten für Privatkunden. Neuigkeiten gab es auch bei Bezahlverfahren. So kündigte TIM eine Lösung für mobiles Bezahlen in Italien an, und Vodafone startete einen Überweisungsdienst in Afghanistan.

Neue, wenige Funkstandards

Bei den Funkverfahren standen vor allem die 3,5G- und 4G-Standards HSPA (High Speed Packet Access), LTE (Long Term Evolution) und Wimax (Worldwide Interoperability for Microwave Access) im Mittelpunkt. LTE, das künftig zwischen 50 und 200 Mbps übertragen soll, war bei fast allen Netzausrüstern ein Thema. China Mobile hat sich Vodafone und Verizon angeschlossen, um gemeinsam Versuchsnetze dafür aufzubauen. Da den Netzbetreibern die Vielzahl von Standards allmählich zu unübersichtlich wird, forderten Vodafone und T-Mobile die Zusammenführung von LTE und Wimax. Um in großen Gebäuden die UMTS-Versorgung zu verbessern, propagieren die Ausrüster schon seit Jahren Pico- und Femtozellen, doch spielten bislang die Netzbetreiber nicht mit. Mittlerweile haben immerhin O2 und Vodafone Versuche damit angekündigt.

Nicht nur schneller sondern auch preiswerter soll die mobile Datenübertragung werden. So kündigten O2 und Vodafone kurz nach der Veranstaltung an, die Verbindungspreise im In- (Vodafone) beziehungsweise Ausland (O2) zu senken. So kosten Vodafones Websessions ab 1. April in Deutschland nur noch 6,68 € pro Stunde. O2 bietet ein 100 MByte großes Datenpaket für 42 € an. Der Tarif gilt für alle Partnernetze des Unternehmens.

Auf den Erfolg des iPhone reagieren viele Hersteller mit verbesserten Bedienkonzepten. Vom Touchscreen über den optischen Joystick oder ein Zweitdisplay unterhalb des Hauptdisplays bis zur QWERTY-Tastatur war auf dem Mobile World Congress alles zu sehen. Doch viele Hersteller haben noch nicht verstanden, dass es um eine einfache und intuitive Bedienung geht. Statt eine ausgereifte Eingabemethode zu integrieren, rüsten sie oft das Gerät mit mehreren Alternativen aus, von denen keine wirklich optimal funktioniert. Immerhin hat Nokia den ersten Prototyp eines Symbian-S60-Geräts mit Touchscreen vorgestellt. Dies zeigt, dass es nach Alternativen zur antiquierten Zifferntastatur sucht.

Android nur auf dem Board

Obwohl Google nicht mit einem eigenen Stand auf dem Mobile World Congress vertreten war und auch noch kein marktreifes Android-Handy vorgestellt hat, konnte man bei verschiedenen Herstellern wie Freescale, Marvell, NEC Electronics, Qualcomm und Texas Instruments Prototypen von Android-Implementierungen auf ARM-Prozessoren sehen. Während einige bereits wie echte Handys aussahen, lief bei anderen das Android-System noch auf einem Entwicklungsboard.

Sony-Ericsson erregte vor allem mit der Ankündigung seines Windows-Mobile-Smartphone Xperia X1 Aufsehen. Es ist mit Touchscreen und ausziehbarer QWERTY-Tastatur sowie mit HSPA und aGPS ausgestattet. Dies überraschte umso mehr, als Sony-Ericsson bei Smartphones bisher immer auf Symbian gesetzt hatte. Die Firma kündigte neben anderen Neuvorstellungen an, bis zum Jahr 2011 die Nummer drei auf dem Mobilfunkt-Markt sein zu wollen.

Weitere Neuigkeiten gab es von Microsoft, das den Gerätehersteller Danger gekauft hat und damit in den Consumer-Gerätebereich einsteigen will. Asus, hierzulande für seine Notebooks bekannt, wird seine Smartphones in Zukunft in Europa anbieten und stellte eine Reihe von Windows-Mobile-Geräten vor. Einem anderen Trend folgt der indische Hersteller Spice, der ein Handy für 20 US-Dollar ohne Display vorstellte und zahlungsschwache Kunden dafür interessieren will. Modu hingegen bietet ein Mini-Handy an, das sich als Modul in verschiedene Hüllen stecken lässt, die dann weitere Funktionen oder ein größeres Display bereitstellen. (ck)

Sicherheit im Deutschen Forschungsnetz

Gut behütet

Dirk Wetter

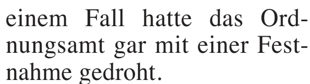
Zum bereits 15. Mal richtete das DFN-Cert seinen Workshop „Sicherheit in vernetzten Systemen“ aus und machte erneut klar, dass Sicherheit mindestens so viel mit Einstellung wie mit Technik zu tun hat.

Rund 300 Zuhörer kamen zur Jubiläumsveranstaltung in die Hansemetropole Hamburg. Ersatz-Keynote-Sprecher Frank Rieger vom CCC widmete sich den Risiken elektronischer Wahlverfahren. Zentrales Thema waren die mittlerweile aus ihrem Heimatland Holland verbannten NEDAP-Computer, die hierzulande im Einsatz sind.

Die verwendete „Old-School-Technik“ erlaubt bei physischem Zugang den 68k-basierten Wahlcomputer zu hacken, zum Beispiel dank der beiden gesockelten und damit leicht austauschbaren EEPROMs, was der CCC anhand von Videos demonstrierte, die auf Youtube zu sehen sind. Als Steuerungssoftware kommt Windows zum Einsatz, gesichtet hatten Wahlbeobachter sogar private Laptops mit XP und lediglich SP1. Der NEDAP-Computer bietet einen hart verdrahteten Wartungsmodus, der bei den niederländischen Geräten durch das Passwort *GEHEIM* aktiviert wird, in der deutschen Version *LOESJE*, ein holländischer Frauenvorname.

Trotz allem hielten die PTB und das BMI an NEDAP fest. An Wahlmanipulationen haben eher Innentäter – nämlich Politiker – als Außentäter ein Interesse. Daher sei es verwunderlich, dass ein Parteimitglied in seiner Privatwohnung über Nacht Wahlcomputer lagerte sowie der CCC auf unbewachte, in Schulen früh morgens vor der Wahl abgestellte NEDAP-Maschinen traf. In einem Fall, so Rieger, kam morgens vor der Wahl ein Transporter vorgefahren, der Fahrer stieg aus und übergab den verdutzten Wahlbeobachtern vom CCC die NEDAP-Computer mit dem Kommentar „Ach, Sie sind die Wahlhelfer“, stieg in seinen Transporter und brauste wieder davon.

Der Keynote-Sprecher vom CCC beklagte, dass viele Wahlhelfer und Wahlleiter wohl nicht über das Grundrecht der Wahlbeobachtung Bescheid wissen. Nicht selten habe die Anwesenheit der CCCler zu Konflikten geführt, die manchmal erst der angerufene Landeswahlleiter klären konnte. In einem Fall hatte das Ordnungsamt gar mit einer Festnahme gedroht.



Wer suchet, der findet

Andreas Schuster (Deutsche Telekom AG) berichtete über File-Carving-Techniken. Solche Standardmethoden zum Wiederherstellen von Dateien, deren Metadaten (etwa Verzeichniseinträge) verloren gegangen sind, orientieren sich in der Regel an „Magic Bytes“ am Dateianfang und bestenfalls am Ende. Das führt stets zu Schwierigkeiten mit Einschlüssen aus fremden Dateien und Dateifragmentierungen. Je nach Carver fallen dabei Datenmengen von mehr als dem 20-Fachen des ursprünglichen Datenvolumens an. Neuere Methoden gehen *in-line* vor – *in-place* und *zero space* werden synonym verwendet.

Statt die Daten zwischen Anfang und dem angeblichen Ende zu kopieren, notieren In-Place-Carver nur diese Positionen und markieren den Bereich als Teil der entsprechenden Datei. Das unter Linux verwendete CarvFS (FUSE) macht die Dateien mittels eines weiteren Werkzeugs (*scalpelcp*) transparent auf der Arbeitskopie verfügbar.

Alexander Geschonneck (HiSolutions AG) berichtete über forensikrelevante Neuigkeiten in Windows Vista, angefangen von neuen Systempfaden und der virtuellen Registry im Benutzerverzeichnis über die wie unter Windows 2003 fehlende einfache Möglichkeit, \\.*Physical Memory* zu sichern bis zum geänderten Papierkorb-Format (keine *INFO2*-Datei, sondern mit *$R* und *$I* beginnende Dateien).

Als wichtigste Änderung in Vista hat der Registry-Schlüssel *NtfsDisableLastAccessUpdate* von Werk aus nun den Wert 1, das heißt, man kann den Zugriffszeitstempel nicht mehr zur Timeline-Analyse heranziehen. Microsoft entschädige den Forensiker bei jeder Vista-Version, so Geschonneck, durch ein im Dateisystem vorhandenes Backup, die „Volume Shadow Copy“, in der man unter Umständen gelöschte Dateien oder alte Dateiversionen wiederfindet. Allerdings, so steht’s zumindest auf den Microsoft-Seiten, nur in der Business- und Ultimate-Version.

Außerdem hat Vista den Schritt weg vom binären Event-Log-Format zu dem etwas klar(er) lesbaren XML vollzogen: Die Logdatei befindet sich unter *system32\winevt\Logs*, wofür Andreas Schuster einen unter GPL stehenden Parser in Perl anbietet.



Klaus-Peter Kossakowski vom DFN-Cert befindet sich offensichtlich auf der richtigen Seite, sonst wäre sein Hut schwarz.

Der Feind auf meiner Festplatte

Exakt 14 Tage vor dem Bundesverfassungsgerichtsurteil widmeten sich die Vorträge von Christoph Wegener und Dirk Fox dem Thema Onlinedurchsuchungen. Beide äußerten sich kritisch wegen offener juristischer Fragestellungen sowie technischer Aspekte der sogenannten „Remote Forensic Software“ (RFS). Juristisch sei ungeklärt, inwieweit die mit ihrer Hilfe generierten Daten wegen der nicht eindeutigen Zuordnung zwischen Person und Computer vor Gericht verwendbar seien. Auch arbeitet die RFS mit den Originaldaten, was in der Computerforensik zu nicht gerichtsfähigen Beweisen führt.

Technisch sei die zuverlässige Einbringung in ein System äußerst schwierig, da Betriebssystem, Patchstand, verwendete Antiviren- und Firewall-Software, Privilegien des Benutzers, Netztopologie (NAT) und vieles mehr bekannt sein müssten. Ein Upload gewonnener Daten über eine DSL-Verbindung sei genauso auffällig wie ein File Carver, der 100 Gigabytes an Daten analysiert.

Wegener kritisierte zudem die Ziele und das technische Verständnis einiger Politiker im Ausschuss, die sich offenbar zu der Aussage verstiegen hatten, man könne damit ja auch Spammer erwischen. Bleibt zu hoffen, dass diese Politiker spätestens nach dem Urteil der obersten Verfassungsrichter mehr auf die Sachverständigen hören. (un)

Salesforce mit neuen Modulen

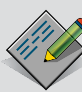
Ihrer CRM-Mietsoftware spendierte Salesforce in der Version Spring 08 zwei neue Komponenten. Mit der ersten namens Content verwaltet der Benutzer unstrukturierte Daten mithilfe von Web-2.0-Techniken wie Tagging, Subskriptionen und Empfehlungen direkt in der Applikation. Die zweite, Ideas, soll den Gedankenaustausch in Gruppen unterstützen und bietet Funktionen wie „My Ideas Inbox“, „Recently Discussed“ und „Top Ideas“. Mit der bereits 25. Release bietet Salesforce die Entwicklungsplattform Force.com zugleich als Dienst über das Internet an.

MID baut Innovator aus

Das Nürnberger Softwarehaus MID hat auf der OOP in München die Version 2008 seiner Modellierungsplattform Innovator vorgestellt. Oberflächen und Zugriffsrechte lassen sich jetzt rollenspezifisch entstellen, und mit einem Traceability Wizard kann der Benutzer Modellelemente miteinander verbinden und pflegen. Der Zusammenhang zwischen Entwurfsanforderungen (Requirements) und Modellelementen soll sich dem Anwender so besser erschließen. MID plant den Austausch von Anforderungen mit einschlägigen Requirements-Werkzeugen über eine RIF-Schnittstelle (Requirement Information Interchange). Diese beruht auf der Vorarbeit der Herstellerinitiative Software (HIS), einer Gründung der deutschen Automobilbranche.

Mit dem Kompositionsstrukturdiagramm, das beispielsweise externe Schnittstellen beschreibt, erhöht sich der Abdeckungsgrad für UML 2.1. Via XMI-Export (XML Metadata Interchange) für UML kann Innovator mit ergänzenden Entwicklungswerkzeugen Daten austauschen. Ebenfalls neu ist der Einsatz von UML-Profilen für die Datenmodellierung. Die Modellierung nach SysML-Standard für eingebettete Systeme ist in Vorbereitung.

KURZ NOTIERT



Einkaufsgelüste: Der niederländische ERP-Anbieter Unit 4 Agresso will Coda Plc übernehmen, einen Hersteller von Programmen für Rechnungswesen und Controlling. Man konnte sich bereits die Zusage für rund 90 % der Aktien sichern. Nach der Fusion käme das neue Unternehmen auf einen Gesamtumsatz von über 300 Mio. Euro.

Modelltour: Intrum Justitia, Dienstleistungsanbieter für Inkasso und Forderungsmanagement, hat seine Legacy-Anwendung Recash Richtung SOA transformiert. Hierzu dokumentierte man mithilfe der Aris Bridge Integration die Applikationsprozesse und überführte den PL/SQL-Code in rund 1000 ausführbare UML-Modelle.

Ausbau: PSIpenta erweitert seine gleichnamige ERP-Suite mit einer Anwendung für das Rechnungswesen. Das neue Modul PSIpenta finance nutzt als Basis die eGecko-Plattform der Fuldaer CSS GmbH. Die Partnerschaft mit der Varial AG, die ebenfalls eine Rechnungswesensoftware im Angebot hat, bleibt davon unberührt.

SCM mit SOA: SAP hat Einzelheiten zur jüngsten Version ihres Lieferkettenmanagements (Supply Chain Management) veröffentlicht. Die kommende Release setzt auf das SOA-Konzept; erweiterte Funktionen liefert SAP als Services aus. So soll es beispielsweise möglich sein, einzelne SCM-Komponenten wie Lieferantenanbindung oder Lagerverwaltung zu nutzen, ohne die gesamte Suite zu installieren. Mitte des Jahres will man das Produkt anbieten.

Quelloffene Datenintegration

Talend, ein Softwarehaus aus Frankreich, veröffentlichte die Version 2.3 der quelloffenen Datenintegrationssoftware Talend Open Studio. Sie bietet ETL-Funktionen (Extract, Transform, Load) für Data Warehouses, eignet sich jedoch vor allem für die Datenmigration und -konsolidierung. Open Studio kann Java, Perl und SQL generieren und benötigt daher keine Ablaufumgebung, sondern lediglich eine Java Virtual Machine oder einen Interpreter. Das Produkt enthält 120 verschiedene Konnektoren und lässt sich mit Datenbanken, Standardanwendungen wie Microsoft Dynamics, Sage oder Mondrian sowie mit POP3-Servern und anderen Zielsystemen verknüpfen. Open Studio soll nicht nur als Konsument von Webservices fungieren sondern auch Datenintegrationsprozesse als Webservice veröffentlichen können. Neben der Open-Source-Variante bieten die Franzosen eine kommerzielle Ausprägung auf Subskriptionsbasis an. Die Integrationssuite verfügt zusätzlich über ein Repository sowie einen Mechanismus zur Steuerung der Integrationsjobs. *Susanne Franke*

Business Objects XI beherrscht Textanalyse

Der kürzlich von SAP gekaufte Business-Intelligence-Anbieter Business Objects hat eine neue Version seiner Auswertungsplattform vorgestellt. Angeblich verfügt Business Objects XI 3.0 als bisher einziges BI-Tool über Funktionen für die Textanalyse. Darüber soll der Anwender die Möglichkeit erhalten, Informationen aus unstrukturierten Quellen wie Internet oder E-Mail in die Analyse der Geschäftslage einzubinden. Reports oder Benchmarks von Finanzinformationsanbietern kann er ebenfalls in seine Auswertungen integrieren.

Diamant/3 unter Windows

Diamant Software erweitert die Rechnungssoftware Diamant/3 um eine Windows-Variante. Bislang lief die .Net-Software lediglich in einem Browser. Unter der Windows-Oberfläche erreicht der Anwender sämtliche Funktionen und Felder auch über Tastenkombinationen. Neu sind Module für die dezentrale Planung sowie die Geschäftsberichterstattung. In die dezentrale Planung lassen sich beispielsweise Excel-Formulare einbinden. Die Controlling-Anwendung kann Daten und Funktionen via Webservices für Excel bereitstellen. Mit Hilfe von Plug- ins ist der Benutzer in der Lage, Menübäume aus Diamant in die Formulare einzuhängen.

Java-Anwendungen als Virtual Appliance

Bea hat sein Virtualisierungsangebot für Java-Applikationen ausgeweitet. Letztere sind nun in der Lage, als eigenständige Appliances auf einer Hypervisor-basierten Virtualisierungsplattform von VMware zu laufen. Virtualization 2.0 umfasst die Middleware Weblogic Server Virtual Edition (WLS VE) und die Managementkonsole Weblogic Operations Control (WLOC). WLS VE enthält eine Ablaufplattform in Form der LiquidVM, die wiederum aus der JRockit-JVM sowie einer dünnen Betriebssystemschicht besteht, zusätzlich einem Weblogic Server und vorgefertigten Deployments.

Via WLOC lassen sich Service Level Agreements (SLAs) überwachen und Anwendungsressourcen dynamisch zuordnen. Agenten verwalten sowohl die virtualisierten als auch die nicht virtualisierten Systemkomponenten. Die Agenten beschränken sich nicht auf WLS VE und können auch mit virtualisierten Java-Appliances umgehen, die nicht von Bea stammen. *Susanne Franke*

Bitkom-Jahreskonferenz
Klimaschutz und Ressourceneffizienz

Low hanging fruits

Barbara Lange

„Klimaschutz und Ressourceneffizienz“ lautete der Titel der Jahreskonferenz, die Bitkom gemeinsam mit dem Bundesumweltministerium und dem Umweltbundesamt Mitte Februar in Berlin durchführte. Ziel war es, IT-Dienstleister und RZ-Betreiber für den wachsenden Energieverbrauch zu sensibilisieren.

Der neue Flaschenhals ist das Fehlen bezahlbarer Rohstoffe“, so Bundesumweltminister Sigmar Gabriel in seiner Eröffnungsrede vor 230 Teilnehmern. Wachsende Industriegesellschaften verbrauchen gigantische Energiemengen – was die Preise explodieren lässt. Dass die ITK-Branche eine entscheidende Rolle beim Schutz des Klimas bei gleichzeitigem Wirtschaftswachstum spielt, darin waren sich alle Redner einig. Auf der Vortragsliste standen Martin Jetter für den Bitkom und IBM Deutschland, Karl-Heinz Florenz für das Europäische Parlament, Molly Webb von der Climate Group (theclimategroup.org) und Dennis Pamlin vom WWF.

Die ITK ist zwar selbst ein großer Stromschlucker, kann aber dank kurzer Innovationszyklen energieeffizientere Materialien, Produkte und Verfahren in „zeitlich spürbaren Zyklen“ entwickeln.

Was man mit den derzeit verfügbaren Mitteln erreichen kann, diskutierten die Teilnehmer in vier parallelen Foren. Insgesamt ließen sich damit nach Angaben des Umweltbundesamtes bereits jetzt 6 Mio. t CO_2 einsparen. Allein die Umstellung eines Drittels der PCs in Deutschland auf Thin Clients würde pro Jahr 1 Mio. t CO_2 und rund 100 000 t Material wie Metalle und Kunststoffe sparen.

Tenor im Forum „Energieeffiziente Rechenzentren“: Nach wie vor bestimmt die permanente Verfügbarkeit Planung und Betrieb eines RZs. Da die Energiekonzerne aber wenig Spielraum lassen, sind neue Ideen gefragt – eingefahrene Konzepte funktionieren nicht mehr. So können Unternehmen durch einen konsequenten Einsatz von bereits verfügbaren Komponenten und Verfahren bis zu 50 % Strom sparen.

Energie ist Chefsache

Dazu gehören Virtualisierung, eine Konsolidierung des Serverparks, das Nutzen der RZ-Abwärme für die Heizung und der Außenluft für die Kühlung sowie Windkanäle, kalte und warme Gänge – alles „low hanging fruits“, die es nur zu pflücken gilt. Belegen konnte dies auch Dr. Klaus Fichter mit seiner Studie „Zukunftsmarkt energieeffiziente Rechenzentren“ von 2007.

Ganz oben auf der Stromsparliste steht jedoch eine höhere Raumtemperatur in Rechenzentren. Davon berichtete Harald Rossol, Geschäftsführer der b.r.m. Technologie und Managementberatung in seinem Vortrag. 35 °C beträgt die Temperatur in seinem RZ – jedes Grad spart drei bis fünf Prozent Energie, so sein Richtwert. Für die Cebit kündigte Bitkom einen „Leitfaden für effiziente Rechenzentren“ an. (sun)

Festplattenreigen: Die Kleinen kommen

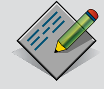
Noch können 3,5 Zoll große Festplatten bei der Kapazität punkten. Doch die kleineren Modelle holen auf. Nach Hitachi hat Fujitsu als zweiter Anbieter ein 2,5-Zoll-Modell mit 500 GByte Kapazität angekündigt. Allerdings passen beide nicht in alle Notebooks: Die hohe Kapazität erreichen die Hersteller nur mit einem 12,5 mm hohen Gehäuse und drei Magnetplatten. Die rotieren in Fujitsus ab Mai lieferbarer MHZ2 BT nur mit 4200 U/min, was die Leistungsaufnahme im Leerlauf auf 0,5 W reduziert. Beim Lesen und Schreiben saugt die Platte 1,8 W aus dem Notebook-Akku.

Toshiba ging bei der 1,8"-Familie MKxx16GSG den umgekehrten Weg und erhöhte die Drehzahl auf 5400 U/min. Die Modelle bringen 120 (MK1216 GSG) beziehungsweise 80 GByte (MK8016GSG) auf jeweils zwei Scheiben unter und sollen bis zu 61 MByte/s übertragen. Beide sind mit einem 1,5 GBit/s schnellen Micro-SATA-Interface ausgerüstet und entsprechen Version 2.6 der SATA-Spezifikation. Im Leerlauf kommen die Platten mit 0,55 W aus, im Ruhezustand mit 0,1 bis 0,45 W. Während des Datenzugriffs steigt die Leistungsaufnahme auf 1,4 W, beim Hochfahren auf 2,5 W.

Von der Kapazität her ebenbürtig sind die Solid State Disks, die das südkoreanische Unternehmen Mtron (www.mtron.net) ab April produzieren will: Die 1,8 Zoll großen Flash-SSDs bringen 128 GByte unter. Beim Lesen sollen sie ihre mechanischen Kollegen mit 110 MByte/s locker abhängen, das Schreibtempo liegt mit 40 MByte/s jedoch deutlich niedriger. Eine geplante Variante mit SLC-Flash (Single-Level Cell) soll 120 beziehungsweise 100 MByte/s erreichen. Preise und Liefertermine stehen noch nicht fest.

Die Performance-Krone gebührt jedoch einer 3,5"-Festplatte: Seagates Cheetah 15K.6. Die Modelle speichern 147, 300 oder 450 GByte auf zwei mit 15 000 U/min rotierenden Scheiben. Damit sollen sie ein Lese- und Schreibtempo von 164 MByte/s erreichen – bei niedrigerem Energiebedarf als die Vorgängermodelle. Die Server-Festplatten mit einer MTBF von 1,6 Mio. Stunden beziehungsweise einer Annual Failure Rate (AFR) von 0,55 % sind mit 3 GBit/s-SAS-Anschlüssen oder 4 GBit/s schnellem Fibre Channel erhältlich.

KURZ NOTIERT



Mischbar: Bereits vor der Cebit kündigte Sun Storagetek seine neue Midrange-Bandbibliothek SL3000 Modular Storage Library an. Sie bietet bis zu 3000 Slots und lässt sich mit bis zu 56 Laufwerken ausstatten. Dabei lassen sich Suns eigene Bandlaufwerke T9840 und T10000 sowie LTO-3- und LTO-4-Streamer von HP und IBM beliebig miteinander mischen. Als Anschlussvarianten stehen Fibre Channel, Escon und Ficon zur Verfügung.

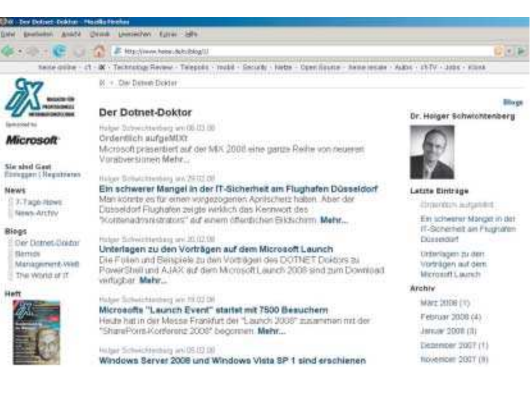
Überarbeitet: HPs erstes Enterprise Virtual Array der 6. Generation heißt EVA 4400. Neue Festplatten-Chassis fassen auf 2 U zwölf FC- oder FATA-Platten mit 146 GByte bis 1 TByte Kapazität. Insgesamt kann das System mit zwei Controllern bis zu 96 Festplatten verwalten, also maximal 96 TByte brutto. Anbindung an die maximal 512 (singlepath) oder 256 (dualpath) Server findet das Storage-System über 2 × 2 FC-Ports und an Tape Libraries über vier weitere.

Vorgeprescht: Während die Hersteller von Grafikkarten an ihren Serienmodellen mit Display-Port arbeiten, beginnt Dell den DVI-Nachfolger-Reigen mit einem Breitbild-Display. Der 30"-Monitor Ultrasharp 3008WFP besitzt außerdem VGA, DVI-D-, S-Video-, Composite- und Component-Anschlüsse und erlaubt eine Auflösung von 2560 × 1600 Punkten.

Prüfungspflichten für Weblog-Betreiber

Das Landgericht Hamburg (Az. 324 O 794/07) hat in der heiß umstrittenen Frage, welche Prüfungspflichten ein Weblog-Betreiber für die Inhalte der Nutzer des Weblog hat, einen neuen Begriff geprägt. Die Betreiber trifft ein sogenannter „gleitender Sorgfaltsmaßstab“ für die Inhaltskontrolle. In Bezug auf rechtswidrige Äußerungen Dritter im Weblog kann das bedeuten, dass, wenn Persönlichkeitsverletzungen mit Sicherheit vorauszusehen sind, eine Pflicht zur Vorabkontrolle fremder Meinungsbeiträge besteht. Ein Weblog-Betreiber stellt Dritten Speicherplatz auf Internetseiten zur Verfügung und ist damit nach den Vorschriften des Telemediengesetzes für sämtliche Inhalte auf diesen Seiten verantwortlich. Daher kann man von ihm die Entfernung einer rechtsverletzenden Äußerung verlangen, wenn er seine Prüfpflichten verletzt hat.

Wann eine Prüfpflicht vorliegt, ist „anlassbezogen“ zu beurteilen. Im konkreten Fall bestand der Anlass darin, dass es zu einer schwerwiegenden Persönlichkeitsverletzung gekommen war, die nach Ansicht der Richter absehbar gewesen sei. Weil der Betreiber dieser Pflicht nicht nachgekommen war, erging eine einstweilige Verfügung gegen ihn. Außerdem hat er die Verfahrenskosten zu tragen. *Tobias Haar*



Ist eine rechtswidrige Äußerung Dritter vorhersehbar, trifft den Weblog-Betreiber die Pflicht zur Vorabkontrolle.

Programmlöschung berechtigt zur Kündigung

Das Sächsische Landesarbeitsgericht (Az. 2 Sa 808/05) hat die fristlose Kündigung eines Arbeitnehmers bestätigt. Dieser hatte auf seinem Firmen-Laptop ein Programm gelöscht, wodurch der Arbeitgeber das Notebook und die Daten darauf nicht mehr nutzen konnte. Der Verpflichtung zur Herausgabe des Laptops kann der gekündigte Arbeitnehmer auch dadurch nicht entgehen, dass er ein neues Programm auf dem Laptop installiert hat und dieses urheberrechtlich gar nicht durch den Arbeitgeber genutzt werden darf. *Tobias Haar*

Kampf gegen Rufnummernmissbrauch

Die Bundesnetzagentur hat erneut einem Unternehmen eine 0900-Rufnummer entzogen, weil damit Rufnummern-Spam für illegale Glücksspiele betrieben wurde. „Missbrauch von Rufnummern und Tricks dürfen nicht Basis für Geschäftsmodelle sein“, sagte Matthias Kurtz, Präsident der Bundesnetzagentur, zu dieser Anordnung. Dem betroffenen Unternehmen wurde ferner untersagt, illegale Telefonwerbung durchzuführen, sowie Rechnungen zu stellen und Forderungen einzutreiben. Das angewandte Geschäftsmodell wurde verboten. Sollte gegen diese Verfügungen verstoßen werden, drohen hohe Zwangsgelder. *Tobias Haar*

Internethändler müssen korrekt verpacken

Seit Kurzem gilt eine Neufassung der Verpackungsverordnung, die die Pflichten von Verkäufern im Hinblick auf Verpackungen der verkauften Waren regelt. Die Neufassung erschwert den Internetversandhandel deutlich: So müssen nun sämtliche Verpackungen, die zu privaten Endverbrauchern gelangen, bei dualen Systemen lizenziert sein. Das gilt aber nicht nur für die Produktverpackungen, sondern auch für Packpapier, Füllmaterial und Versandkartons. Insgesamt soll damit die sogenannte „haushaltsnahe Entsorgung“ über die grünen Tonnen oder gelben Säcke auch für diese Verpackungen gewährleistet werden. Wer sich an diese Spielregeln nicht hält, kann abgemahnt werden. Darüber hinaus drohen Bußgelder für diese Ordnungswidrigkeit von bis zu 50 000 €. *Tobias Haar*

Unternehmen haften für Bannerwerbung

Das Landgericht Frankfurt am Main (Az. 3-08 O 143/07) verurteilte einen Unternehmer, weil er Bannerwerbung auf Webseiten schalten ließ, auf der jugendgefährdende Medien und der Download von Raubkopien angeboten wurden. Das Angebot dieser Webseiten war eindeutig als wettbewerbswidrig einzustufen. Dadurch, dass der Unternehmer, der nicht auch gleichzeitig der Betreiber dieser Webseiten war, auf diesen seine Bannerwerbung schalten ließ, nutzte er den Wettbewerbsverstoß des Betreibers der Webseiten für eigene Zwecke aus. Er profitierte davon, dass viele Nutzer sich auf den rechtswidrigen Webseiten umschauten und dabei seine Werbung zur Kenntnis nahmen. Ihm konnte auch die Verletzung von Prüfungspflichten nachgewiesen werden, da er vor dem gerichtlichen Verfahren auf die Wettbewerbsverletzung hingewiesen und abgemahnt wurde. Trotz dieser Abmahnung ließ er weiterhin seine Werbung auf den Webseiten schalten. *Tobias Haar*

Bundesverfassungsgericht entwickelt Computer-Grundrecht

Im heiß diskutierten Streit um die Einführung sogenannter Onlinedurchsuchungen durch staatliche Strafverfolgungsbehörden hat jetzt das Bundesverfassungsgericht ein wegweisendes Urteil gefällt. Die höchsten deutschen Richter schufen mit diesem Urteil ein „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“. Damit sind alle staatlichen Organe verpflichtet, bei ihren Handlungen, insbesondere auch bei Gesetzesvorhaben, dieses „Computer-Grundrecht“ zu beachten. Das Vorhandensein eines solchen Grundrechts bedeutet aber nicht, dass es nicht auch eingeschränkt werden darf. Gerade bei der Einführung von Onlinedurchsuchungen in den entsprechenden Polizeigesetzen müssen die Verantwortlichen allerdings darauf achten, dass solche Durchsuchungen nur dann erfolgen dürfen, wenn sie verhältnismäßig sind. Auch hier haben die Richter dem Gesetzgeber enge Vorgaben gemacht. Onlinedurchsuchungen sind nur zulässig, wenn eine Gefahr für Leib oder Leben droht oder besteht beziehungsweise wenn die Existenz des Staates gefährdet ist. Außerdem muss ein Richter ihnen vorab zustimmen.

Mit ihrem Urteil erklärten die Karlsruher Richter die Regelungen zur Onlinedurchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig. Dort, in anderen Bundesländern und auf Bundesebene wird es nun neue Gesetzesinitiativen geben, mit denen entsprechende Regelungen in die Verfassungsschutzgesetze, das „BKA-Gesetz“ und die Strafprozessordnung aufgenommen werden sollen. Bundesinnenminister Schäuble kündigte bereits an, in den Gesetzesvorhaben auf Bundesebene die Vorgaben aus Karlsruhe zu berücksichtigen. Die Diskussionen um die geplanten gesetzlichen Maßnahmen werden weitergehen. Am Ende dürfte dann wieder ein Urteil aus Karlsruhe stehen, das feststellt, ob sich die Gesetzgeber an die Spielregeln zur verhältnismäßigen Einschränkung des Computer-Grundrechts gehalten haben. *Tobias Haar*

Geräteabgabe für Multifunktionsgeräte

Multifunktionsgeräte, also Geräte, die in Verbindung mit einem Computer drucken, scannen, fotokopieren und faxen können, unterliegen der urheberrechtlichen Geräteabgabe. Das hat der Bundesgerichtshof entschieden (Az. I ZR 131/05). Seit Anfang 2008 gilt hinsichtlich der Höhe der Abgabe für diese Geräte eine neue Vorschrift im deutschen Urheberrecht.

Diese bestimmt sich nun danach, in welchem Maße die Geräte als Typen tatsächlich für urheberrechtliche Vervielfältigungen genutzt werden. Als Grenze wurde vorgesehen, dass die Abgabe die Hersteller nicht unzumutbar beeinträchtigen darf, und sie muss in einem angemessenen Verhältnis zum Gerätepreis stehen.

Tobias Haar

Fernmeldegeheimnis für gelesene E-Mails

Unter Juristen ist seit Langem umstritten, wann genau das Fernmeldegeheimnis, das auch auf elektronische Kommunikation Anwendung findet, anfängt und wann es endet. Jetzt hat das Landgericht Hamburg entschieden (Az. 619 Os 1/08), dass es für den Schutz von E-Mails nicht darauf ankommt, ob diese noch ungelesen sind und sich noch immer auf dem Server des E-Mail-Dienstleisters befinden oder ob sie schon gelesen wurden und noch auf diesem Server gespeichert sind.

Das Fernmeldegeheimnis soll ungestörte, weil unbeobachtete Telekommunikation gewährleisten, so die Richter. Dazu ist es aber erforderlich, dass E-Mails auch dann diesem Schutz unterliegen, wenn sie (nach erfolgtem Lesen) insbesondere bei Webmail-Diensten auf dem Server des Anbieters gespeichert bleiben.

Nach Meinung der Richter darf bereits deswegen kein Unterschied zwischen gelesenen und ungelesenen E-Mails vorgenommen werden, weil für einen Außenstehenden meist auch gar nicht erkennbar ist, welche bereits gelesen wurden und welche noch nicht.

Tobias Haar

Domains sind Eigentumsrechte nach der Menschenrechtskonvention

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat in einem Verfahren eines Deutschen gegen die Bundesrepublik Deutschland entschieden, dass es sich bei .de-Domains um Eigentumsrechte handelt, für die die Konvention zum Schutze der Menschenrechte und Grundfreiheiten gilt. Das bedeutet aber nicht, dass deutsche Gerichte diesen Schutz nicht einschränken dürfen. Daher unterlag der Kläger im vorliegenden Fall am Ende dennoch. Der Kläger hatte mehrere Tausend Domains auf sich registriert und war unter anderem wegen Namensrechtsverletzungen zur Löschung etlicher Domains verurteilt worden. Dies war nach Auffassung der Richter nicht zu beanstanden, da der Kläger nicht darlegen konnte, wie er „die Domains in nicht rechtsverletzendem Rahmen sowohl gegenüber den Rechteinhabern als auch den Domain-Bedingungen von DENIC zu nutzen gedenke“. *Tobias Haar*

Urteil stärkt Zweifel an Rechtmäßigkeit der Pauschalerfassung

Vorratsklammer

Christoph Wegener, Dennis Werner

Im Urteil des Bundesverfassungsgerichts zum Verfassungsschutzgesetz NRW finden sich Hinweise auf eine Verfassungswidrigkeit der Vorratsdatenspeicherung, die bereits einen Vorgeschmack auf das in diesem Zusammenhang Mitte März 2008 zu erwartende Urteil liefern könnten.

Seit dem 1. Januar 2008 ist das Gesetz zur Vorratsdatenspeicherung (VDS) in Kraft. Es schlägt sich vor allem in den Paragrafen 113a und 113 des Telekommunikationsgesetzes (TKG) nieder und beruht auf der – wegen eines Kompetenzverstoßes – wohl europarechtswidrigen Richtlinie 2006/24/EG. Die bisherige Rechtslage kehrt sich damit vollständig um: Laut § 96 Abs. 2 TKG waren Telekommunikationsanbieter zur sofortigen Löschung aller Verkehrsdaten verpflichtet, die nicht Abrechnungszwecken dienten. Zukünftig sind die Verbindungsdaten sämtlicher Kommunikation für die Dauer von sechs Monaten zu speichern. Das erfasst unter anderem die Rufnummer des Anrufenden und des Angerufenen, im Falle der Mobilfunknutzung zusätzlich die Cell-ID der Teilnehmer-Standorte. Im Rahmen der Internetnutzung wird erfasst, wann wer mit welcher Zugangskennung im Internet aktiv war und wann wer seine E-Mails verschickt, empfangen oder abgefragt hat.

Am 27. Februar 2008 hat das BVerfG nun sein Urteil zum VSG NRW und damit auch zu den viel diskutierten Onlinedurchsuchungen gesprochen (BVerfG, 1 BvR 370/07 v. 27.2.2008). Interessanterweise finden sich in den Randziffern 179 und 183 des Urteils bereits Bezüge zur Vorratsdatenspeicherung. So nennt das BVerfG in Randziffer 179 Persönlichkeitsgefährdungen bei der Internetnutzung, die nicht nur das Auswerten von Kommunikationsinhalten, sondern auch von Verkehrsdaten mit sich bringen kann: „Durch die Speicherung und Auswertung solcher Daten über das Verhalten des Nutzers im Netz können weitgehende Kenntnisse über die Persönlichkeit des Nutzers gewonnen werden.“ In Randziffer 183 wird ausgeführt, das auch die Umstände der Telekommunikation bereits durch Artikel 10 des Grundgesetzes (GG) geschützt sind: „Zudem sind nicht nur die Inhalte […] geschützt, sondern […] auch ihre Umstände. Zu ihnen gehört insbesondere, ob, wann und wie oft zwischen welchen Personen […] Telekommunikationsverkehr stattgefunden hat […].“

Fasst man diese Aussagen zusammen, ergeben sich Widersprüche zu den Regelungen des Gesetzes zur Vorratsdatenspeicherung. Schließlich gebietet diese gerade die Speicherung von Daten, die nach jüngster Auffassung des BVerfG unter anderem durch Art. 10 GG geschützt sind. Komplikationen könnten sich für das BVerfG aus seiner „Solange“-Rechtsprechung ergeben. Demnach ist das BVerfG wegen des Vorrangs des Europarechts in seiner Prüfungskompetenz eingeschränkt, soweit sich das Gesetz im Rahmen der Richtlinie hält. Kein Problem dürfte sich dagegen daraus ergeben, dass im Fall der Vorratsdatenspeicherung die Daten durch private Dritte erhoben werden und nicht wie bei der Onlinedurchsuchung durch den Staat selbst. Hierzu hat das BVerfG bereits im Jahr 2006 klargestellt, dass auch das Speichern von Verbindungsdaten durch private Dritte einen Eingriff in das Fernmeldegeheimnis darstellt. Vor diesem Hintergrund darf das Urteil zur Verfassungsbeschwerde gegen die Vorratsdatenspeicherung mit großer Spannung erwartet werden.



Verbandelt: Ein 12,1-Zoll-Subnotebook von LG mit HSDPA-Modem bietet T-Mobile in Verbindung mit einem Zweijahresvertrag zum Preis von 699 Euro an. Das E200 arbeitet mit einem Pentium Dual Core T2330 (1,6 GHz), 2 GByte RAM und einer 120 GByte großen Festplatte.

Verglichen: Das Team des Virenschutz-Testlabors um Andreas Clementi hat auf www.av-comparatives.org die Vergleichsergebnisse vom Februar zur Verfügung gestellt. Laut Clementi hat besonders Microsofts OneCare darin an Erkennungsrate zugelegt.

Bund plant „Netz des Vertrauens“ auf IPv6-Basis

Das Bundeswirtschafts- und das Bundesinnenministerium haben eine gemeinsame Gesetzesinitiative beschlossen, die Funktion des kommenden, elektronisch auslesbaren Personalausweises zu erweitern. Für „vertrauensvolles Handeln im Internet“ soll jeder Bundesbürger ein persönliches öffentliches IPv6-Netz erhalten, dessen Adressbereich eindeutig mit der Nummer des E-Personalausweises gekoppelt ist. Dieses kostenlos und auf Lebenszeit zugeteilte Netz sollen die Bürger ab einem noch nicht festgelegten Stichtag verpflichtend und ausnahmslos benutzen. Man wartet offenbar nur noch eine ausreichende Durchdringung der Internet-Infrastruktur mit dem neuen Protokoll ab.

Damit entfiele für Provider und Arbeitgeber das Bereithalten eigener Adressbereiche, und dank Mobile IP können die Bürger eigene Adressen vom Handy über das Heimnetz bis zum Arbeitsplatz benutzen. Der E-Personalausweis soll in einer späteren Ausbaustufe darüber hinaus die vertrauenswürdigen Schlüssel für IPSecv6 enthalten und damit eine sichere und verbindliche Kommunikation zwischen Behörden, Bürgern sowie ausgewählten Medienpartnern sicherstellen.

Ein auf diese Weise personalisiertes IPv6 wird nach Ansicht der beteiligten Ministerien die Onlinekriminalität weiter eindämmen. Wenn ein Bürger etwa über seine persönliche IP-Adresse auf ein unregistriertes Onlinekonto zugreift, kann es bereits eine Prüfmeldung ans zuständige Finanzamt geben, noch bevor etwa eine Überweisung erfolgt. Solche Kontrollmeldungen obliegen der Bundesnetzagentur, die zukünftig den deutschen Bürgeradressraum verwalten soll.

Auch auf die Jugendkriminalitätsrate sollen sich die persönlichen IP-Adressen senkend auswirken. So wird das anonyme Tauschen urheberrechtlich geschützter Werke dadurch vollständig verhindert. Wenn Jugendliche illegale Internetdienste einsetzen, könnte die Bundesnetzagentur zukünftig ein Internetverbot aussprechen. Den verbindlichen Bürgeradressraum sehen das Wirtschafts- und das Innenministerium als Meilenstein für den Standort Deutschland und Vorbild für den gesamten europäischen Wirtschaftsraum an. Das persönliche IPv6-Netz soll den Schutz seiner Benutzer vor Internetkriminalität auf ein ganz neues Niveau heben.

Christian Schmidt

KURZ NOTIERT

Kostenloses IT-Grundschutztool: Die Sernet GmbH hat Version 0.6 ihres frei verfügbaren Open-Source-Grundschutz-Tools Verinice veröffentlicht (www.verinice.org). Das für Windows, Linux und Mac erhältliche Werkzeug ist von zertifizierten Auditoren mitentwickelt und bietet in der aktuellen Version den Basis-Sicherheitscheck nach Grundschutz, ergänzende Sicherheitsanalysen und vieles mehr.

Neue BSI-Studien: Sicherheitsaspekte bei Web-2.0-Anwendungen, insbesondere auf der Grundlage von Ajax, behandelt eine Studie des Bundesamtes für Sicherheit in der Informationstechnik. Eine zweite informiert über Log- und Monitoring-Informationen vor allem hinsichtlich ihrer Tauglichkeit für IT-Frühwarnsysteme. Die PDFs sind unter den Stichwörtern „Web 2.0“ und „Logdatenstudie“ unter www.bsi.bund.de/literat zu finden.

Mehr Bankentrojaner: Von den derzeit täglich rund 10 000 neu auftauchenden Schädlingen sind 33 % trojanische Pferde sowie weitere 5 % auf Bankendienste spezialisierte Trojaner. Im vergangenen Jahr ist die Anzahl dieser Banking-Trojaner um fast 500 % von 19 042 (2006) auf 88 165 (2007) gestiegen, meldet Panda Security (www.pandasecurity.com).

a-i3-/BSI-Symposium: Um die Sicherheit von Internetportalen und den Identitätsschutz geht es im gleichnamigen Symposium, das von der Arbeitsgruppe Identitätsschutz im Internet (a-i3) und dem BSI veranstaltet wird. Die interdisziplinäre Expertentagung richtet sich an Mitarbeiter und Verantwortliche aus den Bereichen IT-Sicherheit, Softwareentwicklung, E-Commerce und so weiter. Programm und Anmeldung unter www.a-i3.org.

Workshare bietet Inhaltsschutz für alle Speichermedien

Workshare Protect 6 des fast gleichnamigen Herstellers (www.workshare.com) besteht aus einem Werkzeug-Set für Desktops und Laptops und soll Dokumente sowie Inhalte auf der Grundlage von Policies vor Informationslecks schützen. Eine Clientsoftware lässt sich mit Microsofts Office 2007 und Lotus Notes integrieren und bietet die Möglichkeit, nach inhalteabhängigen Regeln Daten auf Festplatten und mobilen Speichermedien zu verschlüsseln. Eine sogenannte Lightspeed-Engine soll auch versteckte Daten in Dokumenten aufspüren und entfernen, bevor sie das Unternehmen verlassen. Mittels kryptografischer Signatur lassen sich bestimmte Inhalte mit einer überprüfbaren Identität versehen. Das bedeutet, dass diese vertraulichen Informationen beim Management-Modul angemeldet und dadurch, so der Anbieter, von der Software immer als solche erkannt werden, auch falls jemand den Inhalt über Cut-and-Paste in eine andere Datei kopiert.

Eine weitere Komponente, Workshare Protect Network, arbeitet als Hardware-Appliance, kümmert sich um Inhaltsmonitoring sowie -analyse und soll selbsttätig Maßnahmen einleiten, falls sich in der Übertragung befindliche Daten gegen vordefinierte Sicherheitsregeln verstoßen. Diese Maßnahmen können beispielsweise in einer Datenverschlüsselung bestehen. In den Schutz sind auch Endgeräte mit einbezogen, auf denen kein Protect-Client installiert ist. Schließlich gibt es eine Managementkomponente, über die die Regeln zentral erstellt werden sollen und die die Verwaltung der Schlüssel für Festplattenverschlüsselung übernimmt.

Susanne Franke

Sicherheit für VMware-Umgebungen mit Stonesoft-Appliance

Der Sicherheitsanbieter Stonesoft hat seine Firewall/VPN-Appliance für virtuelle VMware-Umgebungen zertifizieren lassen. Die virtuelle Software-Appliance mit einem gehärteten Debian-Betriebssystem und Firewall- sowie VPN-Funktion eignet sich für größere Unternehmen und soll laut Anbieter einfach vervielfacht werden können, um den Datenverkehr an jedem beliebigen Ort zwischen den Servern und Netzwerken in der virtuellen Umgebung zu sichern. Die Appliances, sowohl die physischen als auch die virtuellen, lassen sich zentral über das Stonegate Management Center verwalten und über Policies steuern. Der Anbieter ist kürzlich dem VMware Technology Alliance Partner Program beigetreten, um nach eigenen Aussagen künftige Entwicklungen näher an der Plattform ausrichten zu können. Eine weitere virtuelle Appliance mit IPS-Funktion (Intrusion Prevention System) ist für dieses Jahr geplant.

Für Anbieter von Managed Services und große Unternehmen stellte Stonesoft außerdem zwei neue Produkte vor: Das Intrusion-Prevention-System IPS-6100 und die Firewall FW-5100. Beide Geräte sind für Hochleistungsumgebungen konzipiert und zeichnen sich durch einen hohen Datendurchsatz (IDS 4 GBit/s; FW 10 GBit/s) aus.

Susanne Franke



Forensiksoftware mit verbesserter Suchfunktion

Accessdata (www.accessdata.com), amerikanischer Hersteller von Forensiksoftware, hat nach langer Wartezeit Version 2.0 seines Forensic Toolkit (FTK) veröffentlicht. Mit der neuen Version soll die Arbeit an großen Datenträger-Images leichter von der Hand gehen, da eine Oracle-Datenbank für die Speicherung der Falldaten verwendet wird. Durch die Kombination mit der bereits in der Vorgängerversion 1.7 vorhandenen Suche von dtsearch soll es spürbare Geschwindigkeitsvorteile und noch einfachere Suchmöglichkeiten geben. An Dateisystemen unterstützt das Werkzeug FAT, FAT32, NTFS, EXT2, EXT3, ReiserFS, HFS, HFS Plus, ISO 9660, Ghost und VMware, an E-Mail-Formaten unter anderem MBOX, PST, AOL, DBX, EDB, RFC 822, Hotmail sowie Yahoo.

Die bisher nur über das Passwort Recovery Toolkit separat erhältlichen Passwortanalyse-Funktionen sind nun in FTK enthalten. In der neuen Version soll der Ermittler während des Indexierens weiter am Fall arbeiten können. Mit dem ebenfalls neuen FTK Enterprise führt der Hersteller nun erstmals Clientkomponenten ein, die auch flüchtige Daten sichern sollen – inklusive RAM. Dieses Konzept ist bereits vom Konkurrenzprodukt Encase Enterprise bekannt und bedingt, dass der Agent idealerweise vor dem Sicherheitsvorfall auf das kompromittierte System aufgespielt wurde. Die neue Unicode- und Codepage-Unterstützung ermöglicht die robustere Darstellung aller Unicode-kodierten Sprachen, beispielsweise Arabisch, Hebräisch und des koreanischen Alphabets Hangul.

Alexander Geschonneck

KURZ NOTIERT

Neuer Band: Unter dem Motto „Zwischen freier Software und Gesellschaftsmodell“ hat das Team von der TU Berlin um Professor Lutterbeck das Open Source Jahrbuch 2008 vorgestellt. In fünf Kapiteln setzen sich die Autoren – meist Insider der Community – mit den Aspekten rund um freie Software auseinander. Die PDF-Version gibt’s unter www.opensourcejahrbuch.de, eine gedruckte Fassung wird bei Lehmanns (www.lob.de) erscheinen.

Neuer Besitzer: Sun will seine Virtualisierungsplattform xVM (www.sun.com/xvm) ausbauen und den Anbieter von Open-Source-Virtualisierungssoftware Innotek GmbH übernehmen. Das Produkt Virtualbox unterstützt unter anderem PC mit Windows von 3.1 bis Vista, Linux ab Kernel 2.2, Solaris x86, Netware und DOS; das knapp 20 MByte große Paket steht unter www.openxvm.org zum Download bereit.

Neuer Schirm: Vizekanzler und Bundesaußenminister Frank-Walter Steinmeier hat für den vom 28. bis 31. Mai in Berlin stattfindenden Linuxtag die Schirmherrschaft übernommen. Er unterstreiche damit die Bedeutung von Open Source sowie Linux für den Standort Deutschland und betone zugleich die Wichtigkeit offener Standards für die ungehinderten Informationsaustausch in der globalen Wissensgesellschaft.

Neuer Zweig: Mit der jetzt freigegebenen Version 7.0 haben die Entwickler des FreeBSD-Projekts (www.freebsd.org) eine neue Release-Familie ihres Unix-Derivats freigegeben. Gleichzeitig kündigten sie für Mai an, die offizielle Unterstützung für den 5.x-Zweig einzustellen. *iX* wird sich FreeBSD 7.0 in der nächsten Ausgabe genauer ansehen.

Chemnitzer Linuxtage feiern 10. Geburtstag

Zum inzwischen zehnten Mal fanden dieses Jahr die Chemnitzer Linuxtage (CLT) statt – eine reife Leistung, andere Linux-Veranstaltungen sind längst vergessen. Vermutlich ist die starke Verbindung mit der Community zumindest ein Teil des Erfolgsrezepts, eine Kommerzialisierung findet weiterhin nur sehr dezent statt. Mit immerhin fünf parallelen Sitzungen an zwei Tagen boten die Veranstalter dem Publikum ein prall gefülltes Vortragsprogramm, ergänzt durch einen „Linux Live“ genannten Ausstellungsbereich und weitere Angebote wie Workshops, LPI-Zertifizierungen, eine Key-Signing-Party oder die Praxis Dr. Tux. Erstmals fand auch ein Workshop zum Thema Open Hardware statt.

In seiner Keynote stellte Shane Coughlan von der Free Software Foundation Europe fest, dass Linux und freie Software nun wirklich im IT-Mainstream angekommen seien. Dieser Erfolg verändere jedoch die Community: Es gebe neue Interessengruppen und Diskussionen und einen verstärkten Blick auf die Folgen sowie gesellschaftlichen und kommerziellen Auswirkungen auch außerhalb der „Techie-Community“. Die Herausforderung für die Zukunft sei aber eine andere: Bei allem Erfolg hätten bisher „nur“ eine Milliarde Menschen Zugang zu freier Software, die restlichen fünf Milliarden jedoch nicht.



Michael Weisbach von IBM wagte ebenfalls einen Blick in die Glaskugel. Auch im Lichte der „Green IT“ blieben die Themen Konsolidierung und Virtualisierung aktuell, wobei die Zukunft in komplexen Mischlösungen aus freier und proprietärer Software bestehen würde. Auch Software-Appliances seien wieder im Kommen. Nicht zu unterschätzen sei die neue (im Sinne von anderer) Komplexität der dabei entstehenden Landschaften. Die würde tendenziell, beispielsweise bei SaaS-Konzepten (Software as a Service), größere Anbieter bevorzugen. Wenn sich diese Prognose erfüllen würde, wären dies für viele kleinere Anbieter im Linux-Umfeld schlechte Nachrichten. Frisst die Revolution ihre Kinder? *Christian Böttger*

Open-Source-Konferenz auf der Industriemesse

Im Rahmen der diesjährigen Hannover Messe (21. bis 25. April, www.hannovermesse.de) veranstaltet das Open Source Automation Development Lab (OSADL, www.osadl.org) eG unter dem Motto „Open Source meets Industry“ am 22. April einen Kongress, der sich mit dem Einsatz von freier Software in Embedded-Umgebungen beschäftigen wird.

Für das Programm konnten die Organisatoren eine Reihe namhafter Vertreter der Open-Source-Szene gewinnen. Die Liste reicht dabei von Bruce Perens, Schöpfer des Begriffs „Open Source“, über Kernel-Entwickler wie Alan Cox, Thomas Gleixner, Greg Kroah-Hartman und Andrew Morton bis hin zu Rechtsanwalt Till Jäger, der die juristischen Aspekte des Open-Source-Einsatzes beleuchten wird. Im Vordergrund sollen nicht spezielle technische Entwicklungen stehen, sondern Fragen aus der Praxis des traditionell kommerziell-industriell geprägten Umfeldes. Die Teilnahme kostet 80 Euro (inklusive Messe- und Nahverkehrsticket), die Buchung kann direkt über die OSADL-Webseite erfolgen.

Zwei neue Zarafa-Versionen

Zur Cebit hat Zarafa (www.zarafaserver.de) zwei Varianten seiner Linux-Groupware vorgestellt. So verfügt die neue Version 6.00 neben den obligatorischen Bugfix- und Polierarbeiten über einen Cached/Offline-Modus für Outlook-Clients, einen mehrbenutzerfähigen Kalender für den Webzugriff sowie die vor allem für größere Anwender interessante Option, Attachments in eine separate Datenbank auslagern zu können. Zarafa liefert wahlweise fertige Pakete für Debian, Fedora, Opensuse, Red Hat, SLES und Ubuntu. Die Basis-Variante für fünf Benutzer kostet 300 Euro inklusive Wartung und Updates für das erste Jahr.

Mit der als 6.10 bezeichneten Fassung begibt sich Zarafa auf das Terrain der Hosting-Versionen für den SaaS-Einsatz. Der Hersteller sieht dabei sein neues Multi-Domain-fähiges Produkt als echte Alternative zu Hosted Exchange. Man hofft vor allem über den Preis mit den großen ISPs ins Geschäft zu kommen. Ähnliches gelang Open-Xchange vergangenes Jahr durch seine Kooperation mit 1&1.

Sicherer Webzugang für Unternehmens-PCs

Das neue Produkt Safe Surfer der Sicherheitsfirma Secunet (www.secunet.com) soll das Infizieren von Behörden- und Unternehmens-PCs beim Zugriff auf das Internet verhindern. Dazu wird auf jeden Arbeitsplatzrechner statt des Webbrowsers eine X-Server-Software installiert. Über sie greift der Benutzer nicht direkt auf das Internet, sondern auf einen zentralen Webbrowser zu. Der holt sich die Daten aus dem Internet und liefert dem Client lediglich eine Bildschirmausgabe. Ähnlich funktionieren Druckaufträge: per PDF und E-Mail.

Ergänzt wird die Sicherheitsarchitektur durch eine zwischen Client und Surf-Server sowie Surf-Server und Internet geschaltete Firewall plus Proxy-Server. Weitere Bausteine des Sicherheitskonzepts von Safe Surfer ist das Neustarten des Surf-Servers in individuell definierbaren Intervallen von einem sicheren Medium sowie ein Integritätscheck gegen eine Referenzdatenbank. Bei Angriffen alarmiert Safe Surfer den Verantwortlichen und startet automatisiert eine Neuinstallation des Systems. Potenzielle Schadsoftware wird dabei gelöscht.

Gute Speichergeschäfte – stabile Reihenfolge

Auf ein erfreuliches Abschlussquartal 2007 dürfen die Anbieter von Speichermanagement zurückblicken. Das Marktvolumen weltweit steigerte sich im Vergleich zum Vorjahr um 11,2 % auf 2,9 Mrd. Dollar. Damit lag der Zuwachs knapp ein Prozentpunkt höher als im Gesamtjahr. IDC zufolge führten insbesondere gute Geschäfte im Archivierungssegment zu mehr Wachstum. Mit Blick auf das vierte Quartal führte EMC die Liste der größten Anbieter an, wenn auch der Marktanteil um 1,5 Punkte auf 26 % zurückging. Die folgenden drei Hersteller Symantec (18 %), IBM (12 %) und Netapp (8 %) konnten dagegen ihre relative Marktstellung ausbauen. Dabei wies letztgenannte Firma das mit Abstand höchste Wachstum auf. Eine vergleichbare Entwicklung errechnete IDC mit Blick auf das Gesamtjahr. Wie 2006 führten EMC, Symantec, IBM, Netapp und HP die Liste an. Unter den umsatzstärksten Herstellern war auch hier Netapp (35 %) der „Wachstumsriese“, während Hewlett-Packard mit 0,5 % das Ende zierte.

iX-Umfrage: Cebit-Besuch? Nein, danke!

Wenig Gegenliebe erfuhr die weltgrößte Computermesse bei den Teilnehmern der *iX*-Umfrage, die parallel zu Ausgabe 3/08 lief. Satte 43 % hielten einen Besuch auf dem hannoverschen Messegelände für Zeitverschwendung, 33 % gaben an, ihnen fehle die Zeit. Nur 18 % opferten einen oder mehrere Tage für die ITK-Show (Details siehe Grafik).

Dieselbe Frage war auch im Vorjahr gestellt worden; gegenüber den 2007er-Ergebnissen ist die Cebit-Akzeptanz immerhin um ein paar Prozentpunkte gestiegen – was ja durchaus mit den gestiegenen Besucherzahlen korreliert.

Am 19. März startet auf www.ix.de eine neue Umfrage, Thema: Laptop vs. stationärer PC.



Freenet-DSL vor dem Verkauf

Vorstand und Aufsichtsrat der Freenet AG haben beschlossen, das DSL-Geschäft und das Portalgeschäft in zwei neu zu gründende Tochtergesellschaften auszugliedern. Versatel-Chef Peer Knauer soll bereits Interesse an einer Übernahme des DSL-Geschäftes bekundet haben, um einen DSL-Verbund gegen die Deutsche Telekom zu schmieden. Auch über den Kauf der Kölner QSC durch Versatel oder der hinter dem Unternehmen stehenden Apax Partners wurde bereits spekuliert.

Anschluss-Entbündelung macht Fortschritte

Anfang März hat die Telekom endlich ihre Preisvorstellungen für den entbündelten IP-Bitstream-Access (IP-BSA) bei der zuständigen Regulierungsbehörde, der Bundesnetzagentur, eingereicht. 24,76 Euro pro Monat möchte man als Mietpreis für das „entbündelte DSL“ erhalten, das Konkurrenten ohne Infrastruktur die Chance eröffnet, ein DSL-Angebot ohne Telefonanschluss-Zwang einzurichten. Innerhalb von zehn Wochen will der Regulierer nun eine Entscheidung fällen.

T-Systems findet Partner

Der Telekom-Bereich T-Systems ging Anfang März eine weitgehende Kooperation mit dem US-Pendant Cognizant ein. Diese Partnerschaft „verbindet einen US-Dienstleister mit starken Wurzeln im indischen Markt und einen der führenden europäischen Anbieter“, wird offiziell gejubelt. Beide Firmen bündeln ihr Beratungsgeschäft für Projekte bei Unternehmen mit Offshore-Kapazitäten in Asien und liefern weltweit gemeinsam. Die lange Suche nach einem Partner hat damit letztendlich doch noch zum Erfolg geführt.

Vor allem europäische Firmen sollen von der größeren geografischen Reichweite bei Projekten vor Ort, vom breiteren Service-Angebot und dem weltweiten Zugang zu IT-Kräften profitieren. Über 40 000 Mitarbeiter beider Unternehmen arbeiten off-shore. Insgesamt vereinen T-Systems und Cognizant rund 110 000 Mitarbeiter weltweit. Als Teil der neuen Geschäftspartnerschaft wird die indische Niederlassung von T-Systems mit rund 1150 Mitarbeitern an Cognizant gehen. In den Regionen soll der jeweils stärkere Partner bei den Projekten federführend sein.

Nach Ausführungen von T-Systems-Chef Reinhard Clemens sei die Partnerschaft „faktisch ein Joint Venture“, allerdings ohne die Komplexität der sonst notwendigen Strukturen. Die Kooperation mit Cognizant wird zudem Folgen für die im Bereich Systemintegration beschäftigen Mitarbeiter von T-Systems haben, da deren Aufgabe nun zum Teil off-shore erledigt werden soll. Details wollte man aber noch nicht nennen.

T-Systems hatte im vergangenen Jahr einen Umsatzrückgang von 6,9 % auf rund 12 Mrd. Euro zu verzeichnen. Während das Auslandsgeschäft um 7 % auf 2,5 Mrd. Euro zulegte, schrumpften die inländischen Einnahmen um ein Zehntel auf 9,5 Mrd. Euro. Die Ursache dafür bilden insbesondere rückläufige interne Umsätze im Konzern, die um 15,5 % auf 3 Mrd. Euro einbrachen. Das bereinigte EBITDA (Earnings Before Interest, Taxes, Depreciation and Amortization) reduzierte sich um 17,7 Prozent auf 1,1 Mrd. Euro.

Automatisierte Bestandsdatenerfassung

Die kalifornische BDNA hat eine OEM-Partnerschaft mit der USU AG bekanntgegeben. Ähnlich wie bei BMC wird die BDNA-Inventory-Technik die USU-Produktlinie Valuemation im Bereich der Configuration Management Database (CMDB) ausbauen. Künftig lassen sich damit die Daten sämtlicher IT-Güter im Netzwerk scannen, erfassen und automatisch in Valuemation laden. Dort erfolgt ein Abgleich mit einem umfangreichen integrierten BDNA-Produktkatalog.

Webkonferieren statt telefonieren

Die Karlsruher Netviewer AG hat auf der Cebit einige Erweiterungen ihrer gleichnamigen Webkonferenzsoftware vorgestellt. Für den Einsatz der One2meet-Variante im Support steht eine Pre-Chat-Funktion zur Auswahl. Für einfache Anfragen muss der Benutzer damit nicht mehr direkt zum Telefon greifen oder eine komplette Netviewer-(Konferenz-) Sitzung führen. Ebenfalls neu für One2meet-Variante ist die Funktion Web-Calender zum Publizieren von Meeting-Terminen. Das Veröffentlichen eines Webinars kann dabei wahlweise als reiner Event-Link, als Widget zu einer Auswahl an Veranstaltungen oder in Form einer elektronischen Programmzeitschrift (Electronic Program Guide – EPG) erfolgen.

Mit Netviewer Live Presenter haben die Karlsruher nun auch ein Portal für interaktive Live-Veranstaltungen im Programm. Moderatoren lassen sich per Webkamera zuschalten, Fragen und Kommentare der Teilnehmer werden über die Chat-Funktion übermittelt. Des Weiteren soll in Kürze ein Plug-in für Microsofts Office Communication Server (OSC) verfügbar sein, mit dessen Hilfe sich Netviewer-Sitzungen direkt aus OSC starten lassen. Zusätzlich zum normalen Windows-Arbeitsplatz enthält die Webkonferenzsoftware einen einfachen Browser-Zugang mittels Flash. Er verfügt nicht über alle Funktionen der dedizierten Programme, unterstützt zum Beispiel keinen Dateitransfer.

Computer-Maus intuitiv bedienen

Ein kleines Zeigegerät, das der Anwender wie einen Stift zwischen Daumen und Zeigefinger führt, hat die neuseeländische Firma Simtrix entwickelt (www.simtrix.co.nz). Je nach eingestelltem Modus kann man mit der Maus Kopier- oder Verschiebeaktionen durchführen. Ein weiterer Modus erlaubt es, freie Linien zu zeichnen und zu schreiben. Die Maus lässt sich nicht nur auf dem Schreibtisch bedienen, sondern auch auf einer Laptop-Tastatur. Simtrix hofft, bald Hersteller mobiler Geräte dafür gewinnen zu können, die Swiftpoint-Technik in ihre Systeme zu integrieren.



KURZ NOTIERT

Neues Feld: Trend Micro betätigt sich neuerdings mit seinem „Message Archiver“ auf dem Gebiet der Speicherlösungen. Mitarbeiter sollen mit seiner Hilfe schnellen Zugriff über ihren gewohnten Mailer auf alle archivierten E-Mails bekommen können.

Wachstum: Rund 10 Millionen Kundendomains sind bei 1&1 nach eigenen Angaben derzeit registriert, je zur Hälfte auf Privat- und auf Geschäftskunden. Das bedeutet eine Verdoppelung innerhalb der vergangenen drei Jahre.

Entwendet: Finjan hat nach eigenen Angaben eine in kriminellen Kreisen kursierende Datenbank mit den gestohlenen Zugangsdaten für mehr als 8700 FTP-Server aufgespürt.

Joseph Weizenbaum: „Dissident und Ketzer der Informatik“



Im Alter von 85 Jahren ist Joseph Weizenbaum in Potsdam gestorben. Mit Büchern wie „Die Macht der Computer und die Ohnmacht der Vernunft“, „Kurs auf den Eisberg“ und „Computermacht und Gesellschaft“ war Weizenbaum ein profilierter Kritiker der zunehmenden Abhängigkeit der Gesellschaft von immer komplexeren Computersystemen.

Joseph Weizenbaum wurde 1923 als zweitältester Sohn eines Handwerkers in Berlin geboren, die jüdische Familie emigrierte 1936 in die USA. Als Einwanderer durfte er im Zweiten Weltkrieg nicht bei der Waffentechnik dienen, sondern wurde zum Meteorologen ausgebildet. Nach dem Krieg studierte er Mathematik und konstruierte an der Universität Detroit ein Computersystem für Wetteranalysen. Danach folgten Positionen bei Bendix Aviation und General Electric, wo Weizenbaum verschiedene Computersysteme entwickelte. 1963 erhielt er einen Ruf an das Massachusetts Institute of Technology, wo er die junge Wissenschaft der Computer Science mitbegründete. Wissenschaftliche Meriten erwarb sich Weizenbaum mit Studien zu SLIP (Symmetric List Processor), einer Konkurrenz zu LISP.

Einem breiten Publikum wurde Weizenbaum durch die Programmierung von „Eliza“ bekannt, einem rudimentären Dialogsystem, das er unter dem Titel „A Computer Program for the Study of Natural Language Communication Between Man and Machine“ der Fachwelt vorstellte. Mit Eliza machte er die Entdeckung, dass Menschen mit Computern „reden“ wollten und ihnen vertrauten. Aus der Erkenntnis, dass Maschinen Macht über die Menschen erhalten, formulierte er eine Generalkritik der Computerwissenschaft, die ohne ethische Maßstäbe den Menschen entmündigt: „Der größte Schaden, den der Computer zur Folge haben könnte, hängt weniger davon ab, was der Computer tatsächlich kann oder nicht kann, als vielmehr von den Eigenschaften, die das Publikum dem Computer zuschreibt. Der Nichtfachmann hat überhaupt keine andere Wahl, als dem Computer die Eigenschaften zuzuordnen, die durch die Presse verstärkte Propaganda der Computergemeinschaft zu ihm dringen.“

Auch nach seiner Emeritierung blieb Weizenbaum seinem Thema treu und bereiste vor allem Europa als „Grabenkämpfer gegen Imperialismus der instrumentellen Vernunft“, wie er es einmal formulierte. Mit dem Fall der Mauer zog Weizenbaum aus den USA in seine Geburtsstadt Berlin um. Bis zuletzt gab Joseph Weizenbaum Vorträge, obwohl ihm die Behandlung einer Krebserkrankung schwer zu schaffen machte.

Zahlreiche Erkenntnisse von Joseph Weizenbaum sind heute Allgemeingut, etwa die Beschreibung der Programmierer-Kultur, die für Außenstehende etwas leicht Irrsinniges hat, oder die Kritik an den überzogenen Versprechungen der künstlichen Intelligenz. Seine Warnungen vor Computern in Schulen, mit denen Kinder im „Chat“ die Sprache verlernen oder die Charakterisierung als „Misthaufen Internet“ brachten ihm den Ruf ein, ein Technikfeind zu sein. Ein falscher Eindruck. Bis zuletzt hatte Weizenbaum seinen Spaß mit Digitalkameras, Mobiltelefonen und der Kommunikation über das Internet, allem Neuen gegenüber aufgeschlossen und bereit, den Unsinn in der Technik zu kritisieren, den er schneller entdeckte als viele Nachgeborenen. Sein letztes Programmierprojekt war „New Eliza“, der Versuch, mittels Skype und einem digitalen Anrufbeantworter einen „simulierten Joe“ für Diskussionen über künstliche Intelligenz zur Verfügung zu stellen. Wer über Skype anrief, diskutierte manchmal mit dem echten Weizenbaum. Diese Gespräche sind nun verstummt, die Themen werden jedoch weiterleben. *Detlef Borchers* (WM)

Rechenzentren virtuell automatisiert

Laut Sun ist das xVM Ops Center, eine Managementlösung für die Virtualisierungsplattform xVM zur Automatisierung von Routinearbeiten im Rechenzentrum, jetzt verfügbar. Mit seiner Hilfe soll der Administrator von einer Konsole aus das ganze Rechenzentrum steuern können. Er führt beispielsweise Firmware-Aktualisierungen durch, findet neue Server und installiert Betriebssysteme darauf oder automatisiert Patches und Updates. xVM Ops Center verwaltet Red Hat und Suse Linux sowie Solaris auf der x86- und der Sparc-Plattform. Die Unterstützung von Windows fehlt hingegen. Das xVM Ops Center ist über die Webseite openxvm.org unter der GNU General Public License 3 (GPLv3) freigegeben. Für die Softwarewartung werden zwischen 100 und 300 Dollar pro Managed Server im Jahr fällig.

Virtuelle und physische Systeme überwachen

Nimsoft hat eine neue Version seiner Managementlösung für das Monitoring von virtuellen Umgebungen vorgestellt. Nimbus for VMware dient der zentralen Überwachung virtueller wie physischer IT-Infrastrukturen. Zu diesem Zweck greift die Verwaltungssoftware direkt auf den Distributed Resource Scheduler von VMware zu und migriert virtuelle Rechner, sobald Performance-Engpässe zum Beispiel die Service-Level-Agreements zu gefährden drohen. Neu sind auch automatische Alarm- und Reportingfunktionen für VMwares Event Logs.

Virtualisierung mangelt es an Management

Weltweit räumen 54 % der Großunternehmen dem Management virtueller Server-Umgebungen einen entscheidenden oder hohen Stellenwert in der IT ein. Jedoch sind nur 45 % davon überzeugt, dass ihre Unternehmen auf diesem wichtigen Gebiet effektiv arbeiten. Das ist eine der Kernaussagen der weltweiten Studie www.ca.com/us/products/collateral.aspx?cid=166635 zum Thema „Management von virtuellen IT-Umgebungen“, die CA in Auftrag gegeben hat. 56 % der Befragten nutzen verschiedene Plattformen und Anbieter für das Management der Server-Virtualisierung. Nur 35 % arbeiten auf einer einzigen Plattform. Für 68 % der Befragten spielt das zentralisierte Management von virtualisierten heterogenen Plattformen oder physischen IT-Umgebungen eine entscheidende oder sehr wichtige Rolle. Für die Studie wurden 300 IT-Manager aus Unternehmen in den USA, Europa, dem Nahen Osten und Afrika (EMEA) sowie dem asiatisch-pazifischen Wirtschaftsraum (APAC) mit mehr als 250 Mio. Dollar Jahresumsatz befragt.

Prozess- und Management-Automatisierung

Die Neu-Isenburger Matrix42 AG, die seit Januar nahezu vollständig der Asseco Germany gehört, hat das eigene Produktportfolio durch Kooperationen und wechselseitige Zertifizierungen ausgebaut. So schloss man eine Allianz mit Thinstall, einem Entwickler der gleichnamigen Plattform für Applikationsvirtualisierung. Das erlaubt Matrix42 und seinen Wiederverkäufern, Thinstall direkt anzubieten. Durch die Kombination der Virtualisierungssoftware mit der Managementsoftware Empirum Suite entsteht eine Plattform für das Management der System-Upgrades und Software-Installation, die Stabilität und Integrität einer Desktop-Umgebung gewährleisten soll. Neu ist auch die per Zertifikat bestätigte Integration zwischen Empirum und der Software-Suite von update4u zum Automatisieren der organisatorischen und kaufmännischen Prozesse des IT-Service-Managements.

IT-Freiberufler verdienen mehr

Die IT-Freiberufler in Deutschland profitieren einer aktuellen Analyse des Projektportals Gulp zufolge weiterhin vom Fachkräftemangel. Im Durchschnitt können sie in diesem Jahr nach einem abermaligen Anstieg bei Projekteinsätzen 71 € pro Stunde verlangen. So fordert mittlerweile jeder fünfte IT-Selbstständige (21 %) ein Honorar zwischen 80 und 99 €. Immerhin 8 % der IT-Experten verdingen sich erst ab einem Stundensatz von 100 €. Nach Tätigkeiten aufgeschlüsselt profitierten Projektleiter am stärksten; sie erhöhten ihr Durchschnittshonorar von 76 auf 78 € verbessert haben sich auch Berater (auf 74 €), Trainer (67 €), Softwareentwickler (64 €) und Qualitätssicherungsexperten (63 €). Einzig die Administratoren stagnieren unverändert bei 55 €. Der Honoraranstieg externer IT-Mitarbeiter zieht sich durch fast alle Postleitzahlregionen. Die höchsten Honorare verlangen IT-Spezialisten mit 73 € in Frankfurt am Main und 72 € im Gebiet Düsseldorf–Köln–Bonn, gefolgt vom bayerischen Raum und dem hohen Norden. Bescheidener fallen mit 63 € beziehungsweise 66 € die Forderungen von IT-Selbstständigen aus der Region Halle–Leipzig–Dresden sowie dem Berliner Raum aus. Das Nord-Süd- und zweitrangig das West-Ost-Gefälle bleibt folglich weiter bestehen.

Gehälter in der IT-Branche gestiegen

Laut der Gehaltsanalyse des Online-Karriereportals Monster verdienen Bereichsleiter und Hauptabteilungsleiter in der IT-Branche 2008 deutlich mehr als noch vor zwei Jahren. Arbeitnehmer in diesen Positionen kommen durchschnittlich auf ein Jahresbruttogehalt von 82 000 € was einem Anstieg von 15 000 € gegenüber 2006 entspricht. Auch Berufseinsteiger erhalten mehr: Im Vergleich zu 2006 erhöhte sich das Einstiegsgehalt in 2008 um 6000 € auf rund 37 000 €. Um den gleichen Betrag konnten Angestellten ohne Leitungsfunktion ihre Bezüge auf 48 000 € verbessern. Der hohe Gehaltsanstieg ist nach Ansicht der Portal-Betreiber eine Folge des wachsenden Bedarfs an IT-Fachkräften. Mittlerweile machen auf den Onlineseiten von monster.de und jobpilot.de IT-Jobs fast 20 % aller veröffentlichten Stellenanzeigen aus.

KURZ NOTIERT



Abbruch: Jeder Fünfte bricht das Studium ab. Zu diesem wenig erbaulichen Ergebnis kommt ein Bericht des HIS (Hochschulinformationssystem) mit Blick auf das Einschreibungsjahr 2001. Für Mathematikstudenten (31 %) und Informatiker (32 %) liegt die Rate noch höher.

Preisgeld: Schüler, Studenten und Programmierer können sich am Wettbewerb „THESEUS Talente 2008“ beteiligen und bis zu 10 000 € gewinnen. Der Wettbewerb wird vom Bundesministerium für Wirtschaft und Technologie ausgelobt. Weitere Informationen zum Wettbewerb gibt es unter www.theseus-programm.de, Einsendeschluss ist der 14. April.

Internet Explorer 8: Näher an den Standards

Microsoft hat eine erste Betaversion des Internet Explorer 8 zur Verfügung gestellt. Nach eigenem Bekunden hält sich der Browser genauer an die CSS-Spezifikation 2.1 (Cascading Stylesheets) als seine Vorgänger. So soll er den ACID2-Test bestehen und sämtliche von der Norm vorgesehenen Werte des *display*-Attributs korrekt interpretieren sowie *outline* implementieren. Außerdem bietet er bereits das „Box Sizing“ und vertikalen Text aus CSS3.

Verschwunden ist die *hasLayout*-Eigenschaft, die in Vorgängerversionen das Layout-Verhalten beeinflusste. Statt wie in der Vergangenheit eine *DOCTYPE*-Deklaration für die Auswahl von „Quirks“- und „Strict“-Modus zu verwenden, hat Microsoft jetzt ein eigenes *Meta*-Attribut erfunden. Damit entscheiden Entwickler, ob ihre Webseite wie im Internet Explorer 6, 7 oder 8 aussehen soll.

Auch bei der Unterstützung für Webentwickler will der nächste IE mit seiner freien Konkurrenz gleichziehen. Integrierte Entwicklerwerkzeuge zeigen den DOM-Baum, die jeweils gültigen CSS-Attribute und die Box-Eigenschaften eines Elements an. Außerdem steht ein Javascript-Debugger zur Verfügung. Zumindest in der Beta-Version lassen sich CSS-Attribute jedoch in diesem Werkzeug nicht ändern.

Ähnlich wie Firefox kann der Internet Explorer 8 Schlüssel-Wert-Paare dauerhaft lokal speichern. In Verbindung mit neuen Netz-Events („online“, „offline“) gestattet dies Entwicklern, etwa beim Beenden der Netzverbindung Sitzungsdaten zu sichern. Von maximal sechs gleichzeitigen IP-Verbindungen verspricht sich Microsoft zudem eine Beschleunigung von Ajax-Anwendungen.

Endanwender sollen im neuen IE Teile einer Webseite abonnieren und in der Favoritenleiste ablegen können. Änderungen an der Seite zeigt der Browser dort durch Hervorhebung der URL an. In solche Webslices lassen sich nur die Teile einer Webseite übernehmen, die ihr Entwickler in einen mit *class="hslice"* markierten Container gepackt hat.

Eine einfachere Nutzung des Internet sollen die „Activities“ ermöglichen. Sie sind in XML-Dateien definierte Aktionen, die der Anwender auf dem Dokument oder Teilen davon ausführt. Webseiten stellen diese XML-Dateien bereit, die der Anwender durch Anklicken im Kontextmenü des IE installiert. So könnte man einen unbekannten Begriff in einer Website markieren und durch Rechtsklick auf den passenden Menüeintrag sofort eine Definition dazu suchen lassen.

Studie zur Typologie der Internetkäufer

Gemeinsam mit Wirtschaftswoche und Handelsblatt hat die Hamburger Novomind AG (www.novomind.com) die Onlinestudie „Käufertypologien im Internet – Umsatzstimulation durch erfüllte Kaufmotive“ durchgeführt. 186 Teilnehmer beantworteten Fragen zu Kaufentscheidungen und persönlicher Befindlichkeit in speziellen Kaufsituationen. Bei gut 70 % der Befragten erfolgt die Produktauswahl auf der Basis von Meinungen und Bewertungen Dritter, überwiegend in Foren oder Kundenbereichen von Onlineshops. 54 % orientieren sich bei ihrer Kaufentscheidung an hohen Verkaufsrängen und Benutzerbeurteilungen, während gerade einmal 27 % ihr persönliches Umfeld befragen. Während sich Kunden beim Einkauf im „richtigen“ Laden häufig von Verkäufern unter Druck gesetzt fühlen (16 % der Befragten), empfindet die Mehrheit (70 %) der Umfrageteilnehmer das Kaufen via Internet als angenehm, da sich Online-Empfehlungen, virtuelle Beratung oder Erfahrungsberichte nach Belieben aufrufen lassen. Fast die Hälfte schließlich (43 %) fühlt sich beim Internetkauf freier und weniger bevormundet als bei der Shoppingtour im realen Geschäft.

Interred mit Video

In die auf der Cebit angekündigte Version 10 seines gleichnamigen Content-Management-Systems integriert Interred (www.interred.de) erstmals einen Flash-Player samt Schnittsystem für die Redakteure. Dadurch können sie Videomaterial direkt in dem Format bearbeiten, in dem es später auf der Webseite erscheint. Neue Funktionen erlauben es Nutzern, Beiträge direkt zu kommentieren und selber zu erstellen. Bilder lassen sich nicht nur rotieren, konvertieren und skalieren, sondern auch beschneiden. Für die Druckausgabe unterstützt Interred jetzt Adobes Creative Suite 3 und Quark Express 7.

KURZ NOTIERT

Umfrage zu E-Payment: Welche Zahlungsverfahren Kunden beim Internethandel akzeptieren beziehungsweise aus welcher Auswahl bevorzugen, ist nicht genau bekannt. Im Rahmen des Projekts „E-Commerce-Leitfaden“ führt Ibi Research in Zusammenarbeit mit acht Anbietern von Zahlungssystemen bis zum 30. April eine Umfrage unter Onlinehändlern durch. Teilnahme und weitere Informationen unter www.ecommerce-leitfaden.de/umfrage.

Aktualisiertes Internetrecht: Seit Anfang März steht eine überarbeitete Version des Internetrecht-Kompendiums von Thomas Hoeren online (www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Maerz2008.pdf) zur Verfügung. Der kostenlos abrufbare Text enthält die Rechtsprechung des vergangenen Jahres, das neugefasste Urheberrecht sowie weitere Änderungen.

Vierte Beta von Firefox 3: Der freie Browser nähert sich mit einer weiteren Beta seiner Fertigstellung. Verbesserungen soll es diesmal vor allem hinsichtlich der Leistung, des Speicherbedarfs sowie der Integration in Linux und Mac OS X gegeben haben.

ITK-Markt in Deutschland

Punktlandung

Achim Born

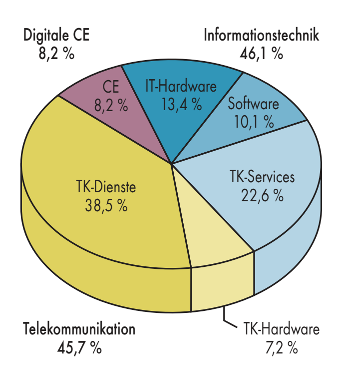
Die Umsätze im hiesigen Markt für Informationstechnik, Telekommunikation und digitale Unterhaltungselektronik entwickelten sich 2007 wie zuletzt prognostiziert. Der alljährlichen Statistik des Bitkom zufolge belief sich das Wachstum auf 2 %. Für das laufende Jahr soll die Zunahme indes geringer ausfallen.

Von der insgesamt guten Konjunkturentwicklung profitierte auch die hiesige ITK-Branche. Bereits zur Cebit 2007 erhöhte der Bitkom die Wachstumsprognose für 2007 von 1,3 % auf 2 %. Ende des Jahres durfte man sich freuen, mit der Vorhersage richtig gelegen zu haben, denn für den „Jahresabschluss“ ermittelt der Branchen-Lobbyverband für den IT-Markt (Informationstechnik, Telekommunikation und digitale Unterhaltungselektronik) ein Gesamtvolumen von 143 Mrd. € und damit ein Plus von 2 %. Für das laufende Jahr soll der Zuwachs jedoch mit 1,6 % im Einklang mit der Gesamtkonjunktur ein wenig zurückgehen. Ein Jahr später, also 2010, soll das Plus wieder 2 % betragen.

Innerhalb des ITK-Markts gibt es derzeit leichte Verschiebungen hin zur Informationstechnik und zur Unterhaltungselektronik. Zurzeit halten die Segmente Informationstechnik und Telekommunikation einen Anteil von jeweils 46 %. Die digitale Unterhaltungselektronik steht für 8 % des Gesamtmarkts. Die Informationstechnik soll dieses Jahr um 4,6 % auf 66,9 Mrd. € wachsen. Für 2009 kündigt der Bitkom ein Plus um 4,4 % auf dann knapp 70 Mrd. € an. Dabei entpuppen sich zum wiederholten Male Software und Services als die eigentlichen Wachstumstreiber. So soll das Marktvolumen im Softwaresegment 2008 rund 14,7 Mrd. € (+5,3 %) betragen. Für 2009 wird ein weiteres Wachstum um 5 % auf 15,4 Mrd. € prognostiziert. IT-Services sollen nach Bitkom-Berechnungen um 6,6 % und 6,5 % auf 32,8 Mrd. € in diesem Jahr und 34,9 Mrd. € im nächsten zulegen. Die Geschäfte mit Computerhardware entwickeln sich nach einigen schwierigen Jahren zumindest stabil auf einem knapp über 19 Mrd. $ liegenden Niveau. Das relative Wachstum weist allerdings nur bescheidene Werte zwischen 0,7 % und 0,3 % auf.

Sorgenkind bleibt indes die Telekommunikation, deren Umsätze im laufenden Jahr mit 66,4 Mrd. € noch einmal um 1,5 % unter dem 2007er-Niveau liegen. 2009 soll sich der Schrumpfungsprozess auf 0,5 % abschwächen, was der Bitkom wohlwollend als „rote Null“ bezeichnet. Grund für die schwierige Marktsituation ist vor allem der anhaltende Preisverfall, der schneller voranschreitet als der Volumenzuwachs der verkauften Telefoneinheiten. Positiv entwickelt sich innerhalb des TK-Markts dagegen die Datenkommunikation. Dieses Segment wächst um jährlich 5 % und federt zumindest teilweise die Verluste in der Sprachtelefonie ab.

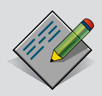
Eingependelt hat sich die Nachfrage nach digitaler Unterhaltungselektronik. Getrieben durch das hohe Interesse an Flachbildfernsehern hat dieser Teilmarkt in den Jahren 2005 und 2006 Rekordzuwächse von 33 % beziehungsweise 19 % eingefahren. Selbst 2007 konnte man mit 8,2 % noch ein überdurchschnittliches Plus auf 11,6 Mrd. Euro erzielen. Die digitale CE wächst weiter, wenn auch eher auf gewöhnlichem Niveau. Für 2008 erwartet Bitkom ein Plus von 2,4 % auf 11,9 Mrd. €, 2009 soll das Wachstum 2,1 % erreichen. Neben Flachbildfernsehern sind es vornehmlich Spielkonsolen und Navigationsgeräte, die die Geschäfte ankurbeln. (WM)



Software AG hegt ehrgeizige Ziele

2007 hat der Darmstädter Software AG das beste Geschäftsergebnis ihrer Unternehmensgeschichte beschert. Der Konzernumsatz betrug 621,3 Mio. € und stieg damit wechselkursbereinigt um 36 %. Die Lizenzumsätze legten währungsbereinigt um 53 % auf 241,3 Mio. € zu. Das EBIT verbesserte sich um 23 % auf 136,8 Mio. €. Den Jahresüberschuss baute die Software AG um 21 % auf 73,2 Mio. € aus. Der Geschäftsbereich Enterprise Transaction Systems (ETS), der hauptsächlich das traditionelle Adabas/Natural-Geschäft zusammenfasst, trug rund 61 % zum Gesamtumsatz bei, die Webmethods-Sparte rund 39 %. Für die Zukunft hat die Software AG ambitionierte Ziele: Im laufenden Geschäftsjahr soll der Umsatz um 24 bis 27 % wachsen, womit die Milliarden-Dollar-Grenze überschritten wäre.

KURZ NOTIERT



Zugelegt: Der Umsatz von Realtech stieg nach vorläufigen Zahlen 2007 um 17 % auf 63,8 Mio. €. Das EBITDA wurde um 49 % auf 7,6 Mio. € verbessert, das Konzernergebnis mit 4,6 Mio. € im Vergleich zum Vorjahr mehr als verdoppelt.

Gnadenlos: Die EU-Wettbewerbskommission verhängte gegen Microsoft eine Geldstrafe in Höhe von 899 Mio. €. Grund ist die Nichtbeachtung der Auflagen des Europäischen Gerichtshofs zwischen März 2004 und Oktober 2007. Die vor Kurzem angekündigte Veröffentlichung der Dokumentationen von Microsoft kam zu spät.

Peu à peu: Der Berliner PSI-Konzern hat nach vorläufigen Berechnungen im Geschäftsjahr 2007 das Betriebsergebnis auf über 3,5 Mio. € gesteigert (2006: 1,0 Mio. €). Der Konzernumsatz erreichte etwa 120 Mio. €.

Oranje boven: Die niederländische ICT ordnet ihre durch Übernahmen kräftig gewachsenen Deutschlandaktivitäten neu. Die hiesigen Betriebsgesellschaften werden in der neuen Holding „ICT Duitsland“ angesiedelt und künftig unter dem Namen „ICT Software Engineering“ agieren.

Back in Black: Medion hat die Wende geschafft. Zierten noch 2006 tiefrote 93,6 Mio. € das EBIT darf sich der Aldi-Lieferant 2007 über ein Plus von 28 Mio. € freuen. Der Umsatz stieg um 3,3 % auf 1,658 Mio. €.

Wechselkurs: Der Umstieg der SAP-Anwender auf die neue Release SAP ERP 6.0 ist in vollem Gang: Mit 37 % setzen 22 % mehr auf die aktuelle Kernlösung von SAP als noch vor einem Jahr. Dies ermittelte die jüngste Online-Umfrage der SAP-Anwendergruppe (DSAG) zum Investitionsverhalten ihrer Mitglieder.

Rangliste der beliebtesten IT-Firmen

Alles beim Alten im Wettbewerb „Deutschlands beste Arbeitgeber 2008“. Wie im vergangenen Jahr erhielten SAP, Cisco und Consol in ihrer jeweiligen Kategorie die Bestnoten als Arbeitgeber. Als Gesamtsieger wechselten Consol und Cisco dieses Jahr die Reihenfolge: Consol führt jetzt. SAP folgt erst auf Rang 18 der von der Mitarbeiterzahl unabhängigen Gesamtliste, deutlich nach Microsoft (Platz 7). Der hiesige Ableger des weltweit größten Softwarehauses konnte aber immerhin den Sonderpreis für „Chancengleichheit der Geschlechter“ einheimsen. Die Rangliste der beliebtesten Arbeitgeber erstellt seit 2002 federführend das Great Place to Work Institute Deutschland. Die Werte zu Qualität und Attraktivität der Firmen als Arbeitgeber werden in einer anonymen Befragung unter den Mitarbeitern zur Glaubwürdigkeit und Fairness der Führungskräfte, zur Identifikation mit der eigenen Tätigkeit und dem Unternehmen insgesamt sowie zur Qualität der Zusammenarbeit ermittelt. Darüber hinaus flossen offizielle Angaben zu den Leistungen, Konzepten und Maßnahmen der Unternehmen im Personalbereich in die Untersuchung ein.

Top 3 der beliebtesten IT-Firmen

Unternehmen über 5000 Mitarbeiter

SAP AG

Dow Deutschland GmbH & Co. OHG

Techniker Krankenkasse

Unternehmen von 501 bis 5000 Mitarbeiter

Cisco Systems GmbH

3M Deutschland GmbH

Impuls Finanzmanagement AG

Unternehmen bis 500 Mitarbeiter

Consol Software GmbH

4flow AG

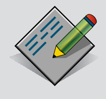
Vedior Personaldienstleistungen GmbH

Quelle: Great Place to Work Institute Deutschland

United Internet schafft gute Jahreszahlen

„Als das erfolgreichste Jahr der Unternehmensgeschichte“ feierte United Internet die Vorlage der vorläufigen Konzern-Geschäftszahlen für 2007. Der konsolidierte Umsatz konnte um 26,7 % auf 1,487 Mrd. € zulegen. Das EBITDA verbesserte sich sogar um 39,6 % auf 308,8 Mio. €. Das Ergebnis vor Steuern stieg kaum weniger stark um 36,9 % auf 234,5 Mio. €. Bis Ende 2007 hatte United Internet mit den Marken 1&1, GMX, Web.de Internetx und Fasthosts 7,23 Millionen Kundenverträge gesammelt, 920 000 mehr als im Vorjahr. Den schwarzen Peter für ein relativ langsames Wachstum bei DSL-Verträgen schiebt man den „zu langen Aktivierungszeiten der Deutschen Telekom bei der Bereitstellung von Hausanschlüssen“ zu.

KURZ NOTIERT



Weiter Verluste: QSC verdoppelte 2007 den Verlust auf 10,1 Mio. €. Immerhin konnte der Kölner TK- und DSL-Provider den EBITDA um 65 % auf 34,9 Mio. € sowie den Umsatz um 28 % auf 335,2 Mio. € erhöhen. Ursprünglich war das Management von einem Gewinn ausgegangen.

Geschafft: Die Beta Systems Software AG erzielte im Geschäftsjahr 2007 eine deutliche Ergebnisverbesserung. Das Betriebsergebnis (EBIT) drehte sich nach vorläufiger Berechnung wieder ins Plus und betrug 5,8 Mio. € (Vorjahr: -15,6 Mio. €). Der Gesamtumsatz ging durch die planmäßige Reduzierung des Hardwaregeschäfts um knapp 10 % auf 88,7 Mio. € zurück.

IDS hält an Wachstumszielen fest

Die IDS Scheer AG hat im Geschäftsjahr 2007 den Konzernumsatz gegenüber dem Vorjahr um 11 % auf 393,5 Mio. € gesteigert. Das Ebita verbesserte sich um 22 % auf 39,6 Mio. €. Der Jahresüberschuss erhöhte sich im Geschäftsjahr 2007 um 25 % auf 23,4 Mio. €. Im Geschäftsbereich Beratung konnte man eine Umsatzsteigerung von 9 % auf 264,1 Mio. € erzielen, die direkten Dienstleistungen im Beratungsbereich wuchsen um 9 % auf 234,7 Mio. €, während die Umsätze mit SAP- und sonstigen Fremdlizenzen sowie die korrespondierenden Wartungserlöse um 16 % auf 29,4 Mio. € zulegten. Die Bereichsumsätze mit Aris-Lizenzen, Wartung und Aris-Services stiegen insgesamt um 15 % auf 129,5 Mio. €, die ARIS-Lizenzerlöse legten um 26 % auf 57,2 Mio. € zu. Zudem investierte man im vergangenen Jahr 13,3 Mio. € in die Forschung und Entwicklung der Aris-Werkzeuge.

Konzerndaten der IDS Scheer

Bereiche	2007	2006
Umsatz Beratung	264,1	241,6
Umsatz Produkte	129,5	112,7
davon Aris-Lizenzen	57,2	45,4
Umsatzerlöse	393,5	354,3
EBITA	39,6	32,6
Konzernüberschuss	22,8	18,2

Angaben in Millionen Euro

Quelle: IDS Scheer, 2/2008

Server-Verkäufe legen zu

Im Schlussquartal vergangenen Jahres erwirtschafteten die Server-Hersteller in Europa, Nahost und Afrika den höchsten je erzielten Quartalsumsatz, seitdem IDC ihren „Quarterly Server-Tracker“ im Jahr 2000 startete. Die Einnahmen lagen mit knapp 5,5 Mrd. $ 3,6 % über dem Vorjahresvolumen. Hierzu mussten die Hersteller allerdings mit rund 750 000 über 7 % mehr Systeme an den Mann bringen. Für das gesamte Jahr 2007 errechnete IDC ein Wachstum von 5,6 % auf 17,86 Mrd. €. Die Auslieferungen legten um 8,9 % auf mehr als 2,6 Millionen Systeme zu.

Mit Blick auf die Prozessoren waren laut IDC im vierten Quartal 2007 knapp 46 % der Server mit x86-CPUs ausgerüstet. EPIC-Prozessoren konnten den Anteil um einen Prozentpunkt auf 8,5 % ausbauen. Nach wie vor die Nummer zwei unter den Prozessoren sind jedoch die RISC-Vertreter mit 30,4 %. Eindeutig die Nummer eins unter den Betriebssystemen ist jetzt Windows bei einem Anteil von 35,7 %. Das Microsoft-System liegt damit drei Prozentpunkte vor Unix. Etliche Federn ließen IBMs proprietäre Offerten im Midrange- und Mainframe-Segment. i5/OS verlor 3,9 % und z/OS sogar 9,1 %.

Ungeachtet dessen behauptete IBM im Schlussquartal die führende Position. Der Abstand zu HP ist allerdings deutlich geschrumpft. Im Gesamtjahresvergleich gelang es Hewlett-Packard jedoch, die zuvor knapp führende IBM zu überholen. Auf den Plätzen drei und vier folgen wie gewohnt Sun und Dell. Letztgenanntes Unternehmen weist von allen Anbietern sowohl für das Gesamtjahr als auch für das Schlussquartal die höchsten Wachstumsraten auf. Wie IBM schloss Fujitsu Siemens Computers, die Nummer fünf im Markt, dagegen das vierte Jahresquartal mit einem Umsatzrückgang bei den Server-Verkäufen ab.

Server-Verkäufe in der EMEA-Region

Hersteller	Umsatz 2006	Marktanteil 2006	Umsatz 2007	Marktanteil 2007	Wachstum
HP	5,412	32 %	6,078	34 %	12,3 %
IBM	5,604	33,1 %	5,580	31,2 %	-0,4 %
Sun Microsystems	1,985	11,7 %	2,092	11,7 %	5,4 %
Dell	1,309	7,7 %	1,508	8,4 %	15,3 %
FSC	1,261	7,2 %	1,283	7,5 %	1,8 %
andere	1,342	7,9 %	1,323	7,4 %	-1,5 %
Gesamtmarkt	16,912	100 %	17,863	100 %	5,6 %

Angaben in Milliarden Dollar

Quelle: IDC, 2/2008



Was die APIs von Amazon, Facebook et al. bieten

Kein Gral in Sicht

Ramon Wartala

Das Web ist das Betriebssystem des Internet, hieß es bei Spiegel Online. Hier hat alles von der Unternehmens-Middleware bis zur Webdienstleistung seinen Platz. Dazu braucht es Schnittstellen für alle, die Webanwendungen schreiben. Der Versuch einer Strukturierung.

Ein Vierteljahrhundert ist es her, dass John Gage und seine Mitstreiter von Sun Microsystems den Slogan „The Network is the Computer“ ausriefen und dabei, niemanden wundert es, als Erstes an die Hardware und nicht an die Mächtigkeit von Software dachten. Heute, über zwei Jahre nach Tim O’Reillys Artikel zum Begriff Web 2.0 (siehe „Onlinequellen“ [a]) dürfte allerdings klar sein, dass Software der eigentliche Schlüssel zum formulierten Versprechen ist. Bei Software as a Service (SaaS), als Nachfolger des Application Service Providing (ASP) in aller Munde, und dem Web 2.0 geht es im Kern um Dienste, die über eines der gängigen Internetprotokolle nutzbar sein sollen.

Obwohl viele schon Anzeichen einer zweiten Blase kurz vor dem Platzen sehen, steckt eine Menge Neues hinter dem, was derzeit Webapplikationen rund um den Erdball anbieten: Programmierschnittstellen jedem zur meist kostenlosen Nutzung zur Verfügung zu stellen. Waren solche APIs (Application Programming Interfaces) in grauer Vorzeit Hilfsmittel, Betriebssysteme und Programmiersprachen für Entwickler verdaulicher zu gestalten, ermöglichen die Programmierschnittstellen moderner Webapplikationen die Nutzung verteilter Dienste, betriebssystem-, programmiersprachen- und hardwareunabhängig.

Schon 1996 wünschten sich Unternehmensberater von Gartner die „serviceorientierte Architektur“ (SOA) herbei, die die Unternehmens-IT in viele kleine solche Dienste unterteilt, die ebenso plattform- wie programmiersprachenunabhängig beliebig zusammenschaltbar sein sollten. Allerdings ist es oft ein langer Weg von der Idee (und dazugehörigen Anforderungen) hin zu ihrer Realisierung.

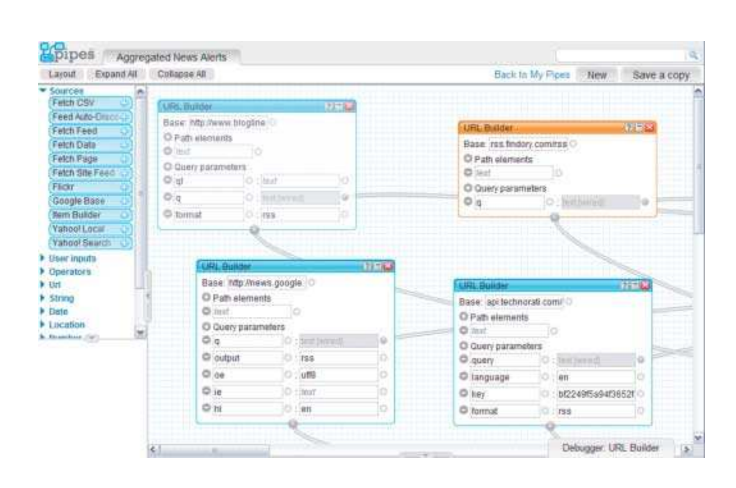
Technik-Kanon in Zeiten des Web 2.0

Mussten Softwareentwickler, -architekten und -entscheider noch vor nicht all zu langer Zeit lediglich mit Frameworks der Basistechniken in Java, .Net und so weiter umgehen können, müssen sie heute ganze Technik-Zoos verstehen und im richtigen Moment einzusetzen in der Lage sein.

Webgestützte Applikationen sind mit vielerlei Techniken implementiert, wobei die Programmiersprache, in der die Anwendung geschrieben ist, zunehmend in den Hintergrund rückt und browserbasierte Techniken eine Renaissance erleben. Javascript beispielsweise hat Netscape schon 1995 als Teil des Navigator eingeführt; die Sprache erfüllt im Web-2.0-Umfeld in Bibliotheksform wie Prototype, JQuery, Scriptaculous und anderen (siehe [2]) eine wichtige Rolle als Klebstoff zwischen Oberflächenelementen und der obligatorischen Ajax-Engine.

Wenn nur wenige Daten mit der unteren Applikationsschicht auszutauschen sind, kommt häufig die Javascript Object Notation (JSON, siehe [3]) zum Einsatz, die das aufwendige Erzeugen und Analysieren von XML vermeiden hilft. XML kommt, wenn überhaupt, meist in den Microcontent-Formaten

RSS oder ATOM zum Einsatz. Daten in Mikroformaten (siehe [1]) erfreuen sich ebenfalls wachsender Beliebtheit. Es handelt sich bei ihnen um speziell angereicherten XHTML-Code, der beispielsweise eine Adresse oder Daten für einen Kalendereintrag enthalten kann. Durch die Annotationen können Fremdprogramme wie Suchmaschinen solche HTML-Daten verarbeiten.



Yahoo Pipes: Visuelle Programmierung von Mashups, die den alten Unix-Gedanken der Pipes spielerisch aufgreift (Abb. 1)

Im Applikations-Backend dominierten bis vor nicht allzu langer Zeit noch proprietäre Protokolle. CORBA, DCOM und RMI waren die Techniken der Wahl zu einer Zeit, als die beteiligten Softwarefirmen noch glaubten, jede für sich hätte den Gral der Middleware entdeckt und könnte diesen fern vom Rest der Welt vermarkten. Dumm nur, dass all diese Objekt-Austauschprotokolle zueinander inkompatibel waren. Schlimmer noch: Sie waren zumeist eng an die präferierte Programmiersprache gekoppelt. Damit begaben sich Nutzer dieser Techniken nahezu vollständig in die Hände der jeweiligen Firma oder, im Falle von CORBA, eines Konsortiums. Das war in Ordnung, solange nur firmeninterne Anwendungen zu integrieren waren. Die Großen der Branche wie IBM und Microsoft registrierten jedoch schon vor der Jahrtausendwende, dass Firmenübernahmen und -zusammenschlüsse im Multimillionenstil nicht zuletzt bei der Migration der Unternehmens-IT immer größere Schwierigkeiten bereiteten.

Ausweg aus der Webservice-Hölle

Ende der Neunzigerjahre haben Entwickler bei Microsoft das Simple Object Access Protocol (SOAP) vorgeschlagen, das das World Wide Web Consortium (W3C) ein paar Jahre später als XML-Lösungsansatz propagierte, um diesem Dilemma Einhalt zu gebieten und Objekte nicht nur über Prozess-, sondern über Applikationsgrenzen hinweg transportieren zu können. Mittlerweile gibt es Webservice Interfaces für eine ganze Reihe von Anwendungsgebieten, die gemeinhin „WS-*“ heißen. Der Stern steht wie üblich als Wildcard für eine ganze Reihe von Funktionen, die man sich im Laufe der Zeit für Webservices erdachte: WS-Trust, WS-Security, WS-Reliability, WSRP und nicht zuletzt der Schnittstellenbeschreibungsdialekt WSDL selbst wurden in den letzten Jahren spezifiziert, implementiert und sicherlich von einigen verstanden und angewendet.

Einfach nutzbarer REST

Doch noch im selben Jahr, in dem sich IBM der Weiterentwicklung von SOAP angenommen hatte, beendete Roy Fielding, einer der HTTP-1.1-Autoren, seine Doktorarbeit mit dem Titel „Architectural Styles and the Design of Network-based Software Architectures“ [b]. Der darin beschriebene Architekturstil „REpresentational State Transfer“ (REST) gilt heute vielen als die Antwort auf die Frage nach einfach nutzbaren Webservice-APIs. Dabei geht es im Kern um die Frage, wie komplex und atomar eine Schnittstelle zu einem Dienst überhaupt sein muss.

Dare Obasanjo, Entwickler bei Microsoft und erfahren im Umgang mit Webservice-Technik, bringt es überspitzt mit der Frage auf den Punkt, wie viele RSS-Feeds Microsoft im Gegensatz zur Anzahl von SOAP-Endpoints produziere [c]. REST-APIs orientieren sich an den Optionen von HTTP und bilden die CRUD-Datenoperationen (Create, Read, Update, Delete) auf die HTTP-Methoden *POST*, *GET*, *PUT* und *DELETE* ab, um auf Daten zugreifen zu können. Und wieder waren es kleine Firmen, die derartige Innovationen schneller in Code gossen als die etablierten der Branche. So erlaubt beispielsweise das Rails-Framework der Firma 37 Signals seit Anfang letzten Jahres die einfache Erstellung von Webapplikationen im REST-Stil [4].

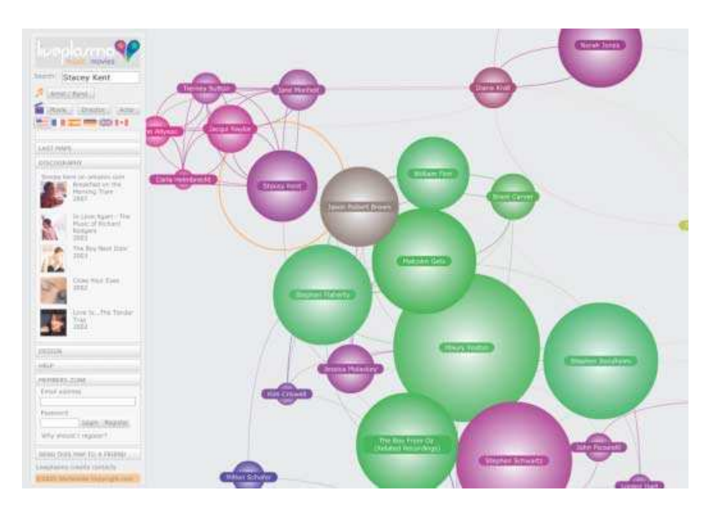
Erst im Mai letzten Jahres präsentierte Pablo Castro von Microsoft auf der MIX 07 die ersten Früchte eines eigenen RESTful-Framework der Softwarefirma aus Redmond. Das auf den Namen Astoria [d] getaufte Projekt soll das unternehmenseigene ADO.Net um einen REST-Ansatz ergänzen. Die Java-Community hat mit dem Java Specification Request 311 [e] und Suns Referenzimplementierung Jersey [f] für den hauseigenen Applikationsserver Glassfish ebenfalls eine REST-basierte Lösung im Angebot. So schließt sich der Kreis zum eingangs erwähnten John Gage. Noch bezeichnender als der späte Einstieg der etablierten Branchengrößen war jedoch, dass den RESTful-Ansatz zuerst Anbieter von Webservices selber propagierten.

Facebooks viele Anwendungen

Yahoos Internet-Fotodienst Flickr war 2005 einer der ersten, der eine REST-API anbot [g]. Services von Paypal, Delicious, Ebay, Google und schließlich Facebook [h] folgten. Der letztgenannte Dienst hat nicht nur durch wilde Spekulationen über den wahren Wert einer derartigen Plattform Schlagzeilen verursacht, sondern vor allen Dingen durch die ständig wachsende Zahl von Anwendungen (über 15 000, Stand Februar 2008), die mit einer mächtigen Programmierschnittstelle [i] erstellt wurden – Anwendungen, die nahezu 60 Millionen registrierte Nutzer [j] innerhalb

iX-TRACT

- Statt Hilfsmittel für Entwickler zu sein, ermöglichen die Programmierschnittstellen moderner Webapplikationen die betriebssystemunabhängige Nutzung verteilter Dienste.
- Webgestützte Applikationen sind heutzutage mit vielerlei Techniken implementiert, wobei browserbasierte Techniken wie Javascript eine Renaissance erleben.
- Der Architekturstil REST gilt heute als die Lösung für einfach nutzbare Webservice-APIs.



Live Plasma: Mashup zeigt Zusammenhänge zwischen Musikern, Filmen und Schauspielern mit Amazons E-Commerce-API (Abb. 2).

ihres Facebook-Profils verwenden können. Da viele der angebotenen Dienste „Wrapper“ um bestehende Webapplikationen sind, sprechen einige schon von Facebook als dem „Betriebssystem des Internet“ [k].

Dass diese pure Masse an online vermarktbaren Menschen nicht nur monetäre Begehrlichkeiten weckt, sondern die schwarzen Schafe der Branche förmlich auf den Plan ruft, zeigte sich Anfang Januar, als eine Facebook-Anwendung Spyware huckepack trug. Bei zahlenmäßig so viel Erfolg wundert es kaum, dass andere Branchengrößen ihre Fälle davonschwimmen sehen. So kündigte Google Ende Oktober letzten Jahres mit der Open Social [l] titulierten API eine Programmierschnittstelle für ein ganzes Konsortium sozialer Netzwerke wie Friendster, LinkedIn, Myspace und Xing an.

Myspace, das zahlenmäßig größte Netzwerk der Google-Initiative, ging am 5. Februar dieses Jahres mit Informationen zur konkreten Implementierung dieser Schnittstelle an die breite Entwickler-Community.

Amazons andere Dienste

Markplätze für Anwendungen können auf Unternehmensebene funktionieren – das hat Salesforce.com als Anbieter eines gehosteten Customer-Relationship-Management-Systems (CRM) mit dem AppExchange getauften Handelsplatz bewiesen [m]. Hier können Firmen Lösungen basierend auf Add-ons und Eigenentwicklungen der Salesforce-Plattform anbieten und einkaufen. Seit 2006 läuft dies sogar mit einer eigenen, auf den Namen Apex getauften, Java-ähnlichen Programmiersprache.

Dienste der ganz anderen Art präsentiert der Onlineversender Amazon in immer kürzeren Zeitabständen. Zuerst nur eine Produktsuche, aber schon bald bot Amazon den Simple Storage Service [n] zur Speicherung von Daten und schließlich die Elastic Compute Cloud [5] zur Anmietung von Rechenleistung als Webservice an. Zahlungsabwicklung und eine einfache Engine zur Speicherung strukturierter Daten namens SimpleDB [o] befinden sich in der Beta-Phase. Produkt-Betas haben die Webservice-Anbieter von den Softwareanbietern der ersten Generation gelernt: schnell eine erste Version des eigenen Produkts zum Anwender bringen, damit dieser begierig die letzten Fehler findet und vielleicht schon Anwendungsfälle konstruieren kann, an die der Produktentwickler gar nicht gedacht hat.

Hier kommen vor allen Dingen die Entwickler sogenannter Mashups ins Spiel, die auf programmableweb.com [p] ein Verzeichnis von Web-APIs und Mashups vorfinden, das derzeit über 590 APIs dokumentiert. Etwas Knowhow vorausgesetzt, kann man aus der Fülle von Diensten eigene Anwendungen „remixen“. Dafür bedarf es nicht unbedingt großer Erfahrungen mit ausgewachsenen Programmiersprachen und eines Servers im Internet. Integrationswerkzeuge wie Yahoos Pipes, Microsofts Popfly oder Googles Mashup Editor [q, r, s] bieten einen einfachen Zugang aus dem Webbrowser heraus; Werkzeugkisten, die die Komplexität bei der Erstellung von Mashups geschickt in mehr oder weniger einfachen, visuellen Metaphern kanalisieren. So mutiert der Nutzer nicht nur zum Lieferanten von Inhalten für soziale Netze, sondern auch zum Erbauer gänzlich neuer Dienste, die durch einfache Verknüpfungen entstehen.

Aus Sicht der API-Anbieter ergeben sich daraus interessante Geschäftsmodelle. In diesem Zusammenhang wird im angelsächsischen Sprachraum schon von Crowdsourcing [t] gesprochen, das die Verteilung der Arbeit auf die breite Masse, in dem Fall der Enthusiasten und Early Adaptors bedeutet.

Dass gerade Mashups als Darreichungsform Kreative anzieht, lässt sich an den zahlreichen Anwendungen sehen, die mit Rich-Media-Techniken wie Adobes Flash oder Microsofts Silverlight andere visuelle Präsentation ermöglichen, als sie von den Entwicklern der eigentlichen Webapplikationen vorgesehen waren. Eine weitere Form der Nutzung bieten sogenannte Widgets auf den unterschiedlichen Systemen an. Auf dem Desktop können die kleinen Helfer in Form von Gadgets für Vista auf Windows-PCs, als Dashboard Widgets auf dem Mac oder mit der Yahoo Widget Engine selbst auf dem Linux-Desktop Dienste von Webanwendungen ausführen [6]. Im Web selber sind dieselben Dienste innerhalb von Content-Management- oder Blog-Systemen als Plug-ins nutzbar.

Mancher mag sich bei all diesen Techniken und Diensten nach dem Warum fragen. Was Firmen motiviert, Derartiges teilweise kostenlos anzubieten – und was Nutzer motiviert, sich wegen dieser Dienste in neue Abhängigkeiten zu begeben. Die Frage nach der Firmenmotivation lässt sich sicherlich leicht beantworten. Im Web regiert ein knallharter Wettbewerb um die Augäpfel der Konsumenten. Jede Firma möchte möglichst viele Nutzer in die eigene Anwendungen locken – aus unterschiedlichen Motivationen, je nachdem, auf welcher Monetarisierungsart das eigene Geschäftsmodell fußt. Das kann von reinen Nutzungsgebühren nach dem bewährten Abo-Modell bis hin zur sprichwörtlich flächendeckenden Vermarktung von Onlinewerbeformen auf der Anwendungsoberfläche reichen.

Kostenlose Dienste können dem anbietenden Unternehmen durchaus Vor-

Copycats – von den USA abgeguckt

USA	Deutschland
Youtube	Myvideo, Sevenload, Clipfish
Myspace	Bloomstreet
Flickr	Sevenload
del.icio.us	Mister Wong
Yelp	Qype
Facebook	StudiVZ
Digg	Yigg, Webnews
Meebo	Mabber
Twitter	Frazr, Wamadu, Baluuu, Niimo
LinkedIn	Xing

teile bringen. Über eine kostenlose, aber nicht informationslose Registrierung gelangen Anbieter von Webdienstleistungen in den Besitz von Bewegungsprofilen, die Inhaber und Nutzer von Bonuskarten im wahren Leben wie träge Couch Potatoes aussehen lassen. Hier lässt sich detailliert jeder Schritt zeitlich, örtlich und sächlich nachvollziehen. Kritischen Naturen seien in diesem Zusammenhang die „Sechs Wahrheiten über freie APIs“ von Nat Torkington [u] ans Herz gelegt.

Vorteile aus Nutzersicht sind dagegen nicht so einfach zu fassen und lassen sich nicht aus der rein kommerziell getriebenen Motivation erklären. Hier geht es zum einen darum, das eigene Ansehen in einer Gruppe zu erhöhen, indem man vielleicht einer der Ersten ist, der eine coole Idee in eine nutzbare Anwendung transformiert hat. Damit bietet sich Raum für selbstreferenzielle Berichterstattung auf dem eigenen Blog, das sich mindestens auf zwei Arten wirkungsvoll vermarkten lässt. Onlinewerbung über Googles Adsense auf renommierten Entwickler-Blogs sind vielleicht Peanuts im Gegensatz zu der Aussicht einer Festanstellung, die ein derartiger Auftritt mit sich bringen kann.

Deutschland versus USA

Der Spruch, dass „die da über dem großen Teich locker zwei Jahre IT-Vorsprung haben“, bestätigt sich wieder, wenn man sich die hiesige Landschaft der Web-APIs ansieht. Nur wenige wagen die Öffnung über nutzbare Schnittstellen wie Imageloop [v] oder Plazes [w]. Dank des allgemeinen Copycat-Gedankens (siehe Tabelle 1), dass jede erfolgreiche, angelsächsische Webapplikation ihr deutsches Ebenbild benötigt, dürften APIs zwangsläufig auch hier zum Renner werden.

Natürlich hat die nahezu unbegrenzte Offenheit dieser schönen, neuen Dienste-Welt ihre Grenzen. Immer noch gibt es Dinge im Netz, die beharrlich auf ihre Standardisierung warten. Dazu gehört beispielsweise ein funktionierendes Bezahl- oder ein Single-Sign-On-System. Hier kochen zumindest alle großen Anbieter weiterhin ihr eigenes Süppchen. Dem Nutzer und letzen Endes Verbraucher all dieser neuen Dienste und Anwendungen kann und darf es nicht recht sein, wenn nur ein Anbieter als Gewinner aus diesem Machtkampf hervorgeht.

In Zeiten wachsender Märkte mag das noch für viele eine andauernde Party sein, die allerdings irgendwann zu Ende gehen dürfte. Die großen der Branche sind vorbereitet – sei es durch prall gefüllte Kriegskassen, die noch die letzten großen Übernahmen (siehe Microsoft und Yahoo) oder den Sprung auf immer neue Plattformen ermöglichen. Seit Jahren schon verspricht das mobile Internet, mit seinen Millionen Handynutzern, das nächste große Ding zu werden. Da erwachen nicht nur die alten Firmen der Vor-Dotcom-Ära wie Microsoft mit Windows Mobile und Apple mit dem iPhone. Firmen wie Google mit Android [7] als offener Mobilfunkplattform und Nokia versuchen, schlagkräftige Allianzen zu schmieden. Allen gemein ist die Hoffnung und die Zuversicht, welche schon die Medienbranche bereichert hat: Durch die Mehrfachverwertung der eigenen Dienste auf großen Plattformen viele Nutzer zu erreichen. (hb)

RAMON WARTALA

ist IT-Leiter beim Hamburger Onlinevermarkter orangemedia.de. Er ist Koautor von „Webanwendungen mit Ruby on Rails“, das 2007 bei Addison-Wesley erschienen ist.

Literatur

[1] Henning Behme; Mehrwert-Markup; Semantic Web von unten; Mikroformate für XHTML, *iX* 11/06, S. 62
[2] Christoph Leisegang, Stefan Mintert, Bastian Spanneberg; Web 2.0; Äpfel und Birnen; Fünf clientseitige Ajax-Frameworks; *iX* 8/2006, S. 54
[3] Sven Neuhaus; Skriptsprachen; Betont schlank; JSON und JSON-RPC: Ajax ohne XML; *iX* 1/2006, S. 70
[4] Thomas Baustert, Ralf Wirdemann; Skriptsprachen; Wieder unterwegs; Ruby on Rails 1.2 mit REST und Unicode; *iX* 3/2007, S. 78
[5] Nathanael Obermayer; Internet; Mehr als einer; Amazon verkauft Rechenleistung mit Elastic Compute Cloud; *iX* 2/2008, S. 64
[6] Henning Behme, Markus Eisele, Stefan Mintert; Desktop-Werkzeuge; Auftritt der Helfer; Widgets für Windows und Mac OS X; *iX* 11/2007, S. 138
[7] Markus Stäuble; Mobiles OS; Komplettpaket; Googles mobile Plattform Android; *iX* 2/2008, S. 34

Onlinequellen

[a] Tim O'Reillys Web-2.0-Artikel
www.oreilly.de/artikel/web20.html
[b] Roy Fieldings Dissertation „Architectural Styles and the Design of Network-based Software Architectures“
www.ics.uci.edu/~fielding/pubs/dissertation/top.htm
[c] Dare Obasanjos „WS-* is to REST as Theory is to Practice“
www.25hoursaday.com/weblog/2007/11/15/WSIsToRESTAsTheoryIsToPractice.aspx
[d] Astoria
astoria.mslivelabs.com/
[e] Java Specification Request 311: The Java API for RESTful Web Services
jcp.org/en/jsr/detail?id=311
[f] Suns Referenzimplementierung des JSR 311: Jersey
https://jersey.dev.java.net
[g] Flickr-API
www.flickr.com/services/api/
[h] Michael Arringtons Facebook-Artikel
www.techcrunch.com/2007/05/24/facebook-launches-facebook-platform-they-are-the-anti-myspace/
[i] Facebook-API
wiki.developers.facebook.com/index.php/API
[j] Facebook-Statistik
www.facebook.com/press/info.php?statistics
[k] Christian Stöcker: Das persönliche Internet
www.spiegel.de/netzwelt/web/0,1518,498946,00.html
[l] Open Social (Google)
code.google.com/apis/opensocial/
[m] Salesforces AppExchange
www.salesforce.com/appexchange/
[n] Amazons Simple Storage Service
www.amazon.com/gp/browse.html?node=16427261
[o] Amazons SimpleDB
www.amazon.com/b/ref=sc_fe_l_2?ie=UTF8&node=342335011&no=3435361&me=A36L942TSJ2AJA
[p] Verzeichnis von Web-APIs und Mashups
www.programmableweb.com/apis/directory
[q] Yahoo Pipes
pipes.yahoo.com/pipes/
[r] Microsofts Popfly
www.popfly.ms
[s] Googles Mashup Editor
code.google.com/gme/tour/tour1.html
[t] Crowdsourcing
www.wired.com/wired/archive/14.06/crowds.html
[u] Nat Torkingtons „Six Basic Truths of Free APIs“
radar.oreilly.com/archives/2007/04/six_rules_for_a.html
[v] Imageloops API
www.imageloop.com/de/api/index.htm
[w] Plazes' API
plazes.com/api/docs



Mit Ebays APIs arbeiten

Jagd nach dem Schnäppchen

Andreas Oesterhelt, Jan Seidler

Seit seiner Gründung vor 12 Jahren hat sich Ebay zu einer der größten E-Commerce-Plattformen entwickelt. Aus technischer Sicht handelt es sich um einen gigantischen Datenbestand, den man über eine Vielzahl von Schnittstellen anzapfen kann. Der Einbau von Markplatz-Daten oder -Funktionen in die eigene Anwendung lohnt sich nicht zuletzt durch die Affiliate-Programme in vielen Fällen.

Ebay ist schon lange ein prototypischer Vertreter des Web-2.0-Modells. Die Firma ermöglicht Interaktion zwischen ihren Benutzern, in deren Verlauf der Datenbestand reicher und für alle Benutzer wertvoller wird. Die öffentlichen Informationen wie Auktionen, Gebote, Bewertungen, Forenbeiträge sind letztlich benutzergenerierte Inhalte. Darüber hinaus kann man weite Teile der Ebay-Sites selbst als Mashup sehen. Auf vielen Seiten der Plattform sind mit üblichen Web-2.0-Techniken kontextverwandte Informationen verwoben.

In den weniger zentralen Bereichen, etwa den Microsites zu speziellen Themen, hat Ebay darüber hinaus schon viele dynamische Ajax-Entwicklungen eingebaut, bis hin zu Seiten, die de facto keinen servergenerierten HTML-Content mehr haben.

Weitreichender Zugriff erlaubt

Über umfangreiche Schnittstellen sowie vielfältige Datenquellen und Services bietet die Plattform Zugriff auf nahezu sämtliche Aspekte des Ebay-Geschehens. Nach ausdrücklicher Zustimmung der jeweiligen Benutzer über ein spezielles, „Auth & Auth“ genanntes Login-Verfahren ist sogar der Zugriff auf ausgewählte persönliche Informationen und Funktionen erlaubt, bis hin zur Abgabe von Geboten oder dem Einstellen neuer Auktionen. Extern bietet beispielsweise die Krefelder Via-Online mit ihrer Software Afterbuy (www.afterbuy.de) eine über die APIs integrierte Lösung für die komfortable, automatisierte Abwicklung von Auktionen, inklusive Rechnungsstellung und Kundendatenverwaltung an.

Tatsächlich werden schon heute über 25 Prozent aller Auktionen über die APIs eingestellt. Monatlich erfolgen über 5,5 Milliarden API-Aufrufe. Da ist es nicht weiter verwunderlich, dass Ebay im Laufe der Jahre nicht nur die technischen Kapazitäten, sondern auch das Angebot an Toolkits, Dokumentationen, Veranstaltungen und Support innerhalb des Entwicklerprogramms konsequent ausgebaut hat. Kernstücke sind die dokumentierten Software Development Kits (SDKs) und Testtools, zu denen eine Sandbox-Testumgebung gehört. Bei Schwierigkeiten während der Entwicklung steht zudem ein technisches Support-Team von Ebay bereit.

Von den APIs ist deshalb im Plural die Rede, weil Ebay die insgesamt über 120 angebotenen Calls auf zwei verschiedene Schnittstellen aufgeteilt hat, die für unterschiedliche Anwendungen optimiert sind. Dabei ermöglichen die Abrufe der Shopping-Webservices, öffentliche Daten auf schnelle, leichte und schlanke Weise abzurufen. Mit dieser API realisieren Entwickler etwa Suchfunktionen über Auktionen, Benutzer, Produkte, Testberichte sowie den Abruf einzelner Angebote oder Benutzer. Der Funktionsumfang befindet sich in ständiger Erweiterung, auch weil die Abrufe der alten REST-API schrittweise hierher migriert werden. Technisch steht die Shopping-API als REST- und als SOAP-Schnittstelle zur Verfügung.



Alles meins: Im Dashboard kann man seine individuelle Sicht auf Ebay zusammenstellen (Abb. 1).

Die ungleich umfangreicheren Trading-Webservices, die ausschließlich über SOAP ansprechbar sind und vielfach Authentifizierung über ein Benutzer-Token erfordern, stellen im Gegensatz dazu zentralere und komplexere Funktionen bereit, die das gesamte Marktgeschehen vom Einstellen von Auktionen über Gebote, Abruf von Transaktionen nach Auktionsende bis zur Bewertung des Handelspartners abdecken. Darüber hinaus lassen sich nahezu alle persönlichen Daten verwalten, etwa die Listen beobachteter, ge- oder verkaufter Artikel. Sogar das Web-Äquivalent von Callbacks ist machbar: Man kann die API bitten, beim Eintreten bestimmter Events aktiv eigene HTTP-URLs aufzurufen.

Marktgeschehen abgedeckt

Bei der Wahl der Sprache ist der Entwickler frei; schließlich tauschen die REST und SOAP-Protokolle nur Textnachrichten aus, die man notfalls in Assembler generieren und untersuchen könnte. Das Herstellen eines eigenen SOAP-Connectors aus den WSDL-Beschreibungen, die das Entwicklerprogramm bereitstellt, ist ebenfalls nicht jedermanns Sache. So fällt die engere Wahl auf Sprachen, für die SDKs existieren: PHP, Perl, Java, C#, Javascript oder Actionscript innerhalb einer Flash-Anwendung. Ebay selbst hat kürzlich beispielsweise unter dem Namen Ebay Desktop eine nur auf Adobe Air und der Ebay API basierende Software fertig gestellt, die ein vollständig neues Benutzer-Interface anbietet.

Doch nicht nur über die APIs lassen sich Daten des Marktplatzes für Web-2.0-Applikationen abrufen. Diverse öffentliche RSS- und XML-Feeds (beispielsweise in den Bereichen Community, Blogs, News und Answer Center) kann ein externer Entwickler ebenso berücksichtigen wie die komplementären Funktionen für Entwickler von Paypal, Shopping.com oder Skype.

Ajax und kein Ende: Das Dashboard

Besonders interessant für Betreiber von Webseiten auf der Suche nach Web-2.0-Inhalten sind die Ebay Relevance Ads, in denen man leicht und schnell im

iX-TRACT

- Mit insgesamt 120 Calls aus zwei APIs erlaubt Ebay externen Entwicklern Zugriffe auf seine Daten – per REST und SOAP.
- Ebay selbst hat mit einer Mischung aus PHP und Javascript ein sogenanntes Dashboard entwickelt, das als Vorbild für kleine Anwendung dienen kann.
- PHP inklusive des von Ebay stammenden EbatNS sowie die Javascript-Bibliothek Prototype und ein bisschen XSLT reichen aus, eine Schnäppchenjagd zu programmieren.

Listing 1: Konfigurationsdaten

```
<?php
/*
[ebay-config]
dev-key-prod = <bitte ergänzen>
app-key-prod = <bitte ergänzen>
cert-id-prod = <bitte ergänzen>
site-id = 77 ; eBay.de
app-mode = 0 ; 1 => sandbox, 0 => production
[ebay-transaction-config]
use-http-compression = 1
*/
?>
```

Rahmen eines Affiliate-Programms passende Werbemittel auf die eigenen Seiten integriert, mit denen der Besitzer wiederum Einnahmen generieren kann.

Es müssen nicht zwangsläufig externe Entwickler sein, die über die API an Ebay andocken. Eine von und für Ebay betriebenen Site, die dennoch über die API zugreift und technisch viele Web-2.0-Register zieht, ist das Ebay-Dashboard. Ursprünglich zur Einbettung in 3rd-Party-Portale entwickelt, bietet es dem Benutzer eine radikal individualisierbare Sicht auf Ebay. Informationen, die sonst auf verschiedenen Unterseiten verfügbar sind, wie die persönliche Beobachtungs- oder Gebotsliste, verbinden sich mit Messaging, RSS-Reader, Suchmöglichkeit inklusive Kartendarstellung des Artikelstandorts und anderen Daten zu einer Sicht.

Die Mittel, mit denen Ebay das Dashboard realisiert hat, sind ein klassischer Ajax-Mix, der auch für die Codebeispiele dieses Artikels Verwendung findet: Server liefern dynamischen Content und die Feeds durch PHP aus, das zu diesem Zweck mit der PHP-Template-Engine Smarty, den einschlägigen PEAR-Modulen sowie zur Anbindung an die Ebay-API (Shopping und Trading) mit dem Accelerator Toolkit for PHP (EbatNS) ergänzt wurde. Für das „rich“ in Rich Client zeichnet neben dem Browser-internen Support für XMLHttpRequest und XSLT vor allem die populäre Javascript-Klassenbibliothek Prototype verantwortlich, in den Bereichen Drag & Drop und visuelle Effekte kommt das Prototype-basierte Scriptaculous zum Einsatz.

Weil Ausprobieren manchmal mehr bringt als Nachlesen (und mehr Spaß bereitet), folgt hier ein Beispiel mit Grundbausteinen aus der Shopping-API: eine Suche nach günstigen Angeboten. Dafür ist ein Feed erforderlich, der zu einem gegebenen Keyword solche Angebote findet, die im Auktionsformat laufen (im Gegensatz zu Festpreis-, Shop- und anderen Formaten), bald enden, und für die noch keine Gebote vorliegen. Auf der Clientseite muss eine Javascript-basierte Infrastruktur vorhanden sein, die den Feed und das Stylesheet anfordern, anschließend die XML-Daten in HTML transformieren und schließlich einen Container innerhalb der Seite dynamisch mit den Ergebnissen befüllen kann. Nicht zu vergessen: das XSLT-Stylesheet für die Transformation.

Futter für die Jagd

Soweit es den Feed betrifft, stellt sich die Frage, warum der Client die Daten nicht direkt über die API beziehen kann – ohne den Umweg über einen Feed-Server, der seinerseits die API-Kommunikation betreibt. Und tatsächlich kann man gänzlich ohne eigene Serverkomponente arbeiten. Dagegen sprechen aber praktische Aspekte. Ein XML-Feed ist nur für XMLHttpRequest-basierte Verarbeitung verdaulich, die aber auf die Domain des aktuellen Dokuments beschränkt ist. Der alternativ verfügbare JSON-Feed wird als *<script>* eingebunden, und ist daher schlecht dynamisch parametrisierbar. In jedem Fall ist das Tracking erschwert und die *AppID* aus dem Key-Tripel für den Client transparent. Der Hauptgrund für einen eigenen Feed ist aber oft, die Daten lokal abgleichen und anreichern zu können.

Für die Schnäppchenjagd soll daher eine stark vereinfachte Variante des Dashboard-Aufbaus zum Einsatz kommen: PHP mit EbatNS (Shopping) für den Feed, Javascript mit Prototype auf dem Client. Nachdem alle nötigen Bibliotheken und Tools beschafft und installiert sind, kann es mit der Implementierung des Feed losgehen. Damit dieser mit der Shopping-API kommunizieren kann, ist zunächst das Key-Tripel nötig. Dieses kann dem EbatNS auf verschiedene Weisen zur Verfügung gestellt werden; am einfachsten in einer Konfigurationsdatei (siehe Listing 1).

Jetzt kann das eigentliche Feed-Skript beginnen und die relevanten Klassen des EbatNS einbinden (Listing 2, Abschnitt 1). Die *ServiceProxyShopping*-Klasse wickelt die API-Kommunikation inklusive Erzeugung von SOAP-Requests und Parsing der Responses und aller nötigen Konvertierungen ab. Aus den API-Responses werden analog strukturierte PHP-Objekte erzeugt, die außer dem Payload alle Metadaten zur XML-Struktur der Response beinhalten, sodass eine Rückkonvertierung jederzeit möglich ist. Analog existieren Klassen, die die Requests repräsentieren und deren Instanzen vor der Übergabe an den Proxy parametrisiert werden können. Der *DataConverter* schließlich dient der Reserialisierung schon analysierter Responses, wie sie bei der Verwendung von API-Results als XML-Feed anfallen.

Zunächst muss das Feed-Skript den *ServiceProxy* instantiieren und mit dem Key-Tripel ausstatten. Zum Einlesen der Konfigurationsdatei dient ein *Session*-Objekt, dessen Konstruktor den Pfad der Datei übergeben bekommt. Die Session wird im zweiten Schritt bei der Erzeugung des Proxy verwendet (Listing 2, Abschnitt 2). Die Parser-Optionen sind nur im Hinblick auf die spätere erneute XML-Serialisierung erforderlich und sorgen für die Erhaltung der Metadaten zum Response-Format und aller leerer Knoten – beides würde sonst

Listing 2: PHP-Feed (6 Abschnitte)

```
<?php
// Abschnitt 1
require_once 'EbatNs/EbatNs_ServiceProxyShopping.php';
require_once 'EbatNs/FindItemsAdvancedRequestType.php';
require_once 'EbatNs/FindItemsAdvancedResponseType.php';
require_once 'EbatNs/EbatNs_DataConverter.php';
// Abschnitt 2
$session = new EbatNs_Session('config.php');
$proxy = new EbatNs_ServiceProxyShopping($session);
$proxy->setParserOption('NO_UNSET_METADATA', true);
$proxy->setParserOption('NO_REDUCE', true);
// Abschnitt 3
$request = new FindItemsAdvancedRequestType();
$request->setQueryKeywords(utf8_decode($_REQUEST['query']));
$request->setEndTimeFrom(date('Y-m-d H:i:s', time() + 120));
$request->setEndTimeTo(date('Y-m-d H:i:s', time() + 86400));
$request->setItemType('AuctionItemsOnly');
$request->setBidCountMax(0);
// Abschnitt 4
$request->setItemSort('EndTime');
$request->setSortOrder('Ascending');
$request->setMaxEntries(5);
$request->setPageNumber(isset($_REQUEST['page']) ? $_REQUEST['page'] : 1);
// Abschnitt 5
$result = $proxy->FindItemsAdvanced($request);
if ($proxy->isGood($result)) {
  $result->_elements['CurrentPage'] = array
  (
    'required' => false,
    'type' => 'string',
    'nsURI' => 'urn:ebay:apis:eBLBaseComponents',
    'array' => false,
    'cardinality' => '0..1'
  );
  $result->CurrentPage = isset($_REQUEST['page']) ? $_REQUEST['page'] : 1;
// Abschnitt 6
  header('Content-Type: text/xml');
  echo('<?xml version="1.0" encoding="utf-8"?>');
  echo
  (
    $result->serialize
    (
      'ebaySearchResults', $result, null, true, null, new
      EbatNs_DataConverterIso()
    )
  );
}
?>
```

Listing 3: XSLT-Stylesheet

```
<?xml version="1.0"?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:decimal-format decimal-separator="," grouping-separator="."/>
  <xsl:template match="/">
    <table cellpadding="0" cellspacing="2" border="0">
      <tr>
        <th>
          Bild
        </th>
        <th>
          Artikelbezeichnung
        </th>
        <th>
          Preis
        </th>
      </tr>
      <xsl:for-each select="ebaySearchResults/SearchResult/ItemArray/Simpleitem">
        <xsl:variable name="zeilentyp">
          <xsl:choose>
            <xsl:when test="position() mod 2 = 1">ungerade</xsl:when>
            <xsl:otherwise>gerade</xsl:otherwise>
          </xsl:choose>
        </xsl:variable>
        <tr class="zeile_{$zeilentyp}">
          <xsl:variable name="ItemLink" select="ViewItemURLForNaturalSearch"/>
          <td>
            <xsl:choose>
              <xsl:when test="GalleryURL">
                <a href="{$ItemLink}">
                  <img height="64" width="64" border="0" src="{normalize-space ↙
                 (GalleryURL)}" alt="{Title}"/>
                </a>
              </xsl:when>
              <xsl:otherwise>
                <a href="{$ItemLink}">
                  <img src="http://pics.ebaystatic.com/aw/pics/de/entertainmentratgeber/ ↙
                 v1/E-Ratgeber_Icon-Bild-weiss_80x60.gif" alt="{Title}" width="80" ↙
                 height="60" border="0"/>
                </a>
              </xsl:otherwise>
            </xsl:choose>
          </td>
          <td>
            <a href="{$ItemLink}">
              <xsl:value-of select="Title"/>
            </a>
          </td>
          <td>
            <b>
              <xsl:value-of select="concat(ConvertedCurrentPrice/@currencyID,' ',↙
              format-number(ConvertedCurrentPrice, '#.##0,00'))"/>
            </b>
            <xsl:if test="ConvertedBuyItNowPrice!='0'">
              <br/>
              <xsl:value-of select="concat(ConvertedBuyItNowPrice/@currencyID, ' ',↙
              format-number(ConvertedBuyItNowPrice, '#.##0,00'))"/>
              <br/>
              <img border="0" title="Sofort-Kaufen" alt="Sofort-Kaufen" ↙
             src="http://pics.ebaystatic.com/aw/pics/de/bin_15x54.gif"/>
            </xsl:if>
          </td>
        </tr>
      </xsl:for-each>
          <tr>
            <td colspan="2">
              <xsl:if test="ebaySearchResults/CurrentPage &gt; 1">
                <span style="cursor: pointer; color: blue;" onclick="findEbayItems ↙
                (null, 'previous')">Zurück</span>
              </xsl:if>
            </td>
            <td colspan="1" align="right">
              <xsl:if test="ebaySearchResults/CurrentPage &lt; ebaySearchResults/TotalPages">
                <span style="cursor: pointer; color: blue;" onclick="findEbayItems(null, ↙
               'next')">Weiter</span>
              </xsl:if>
            </td>
          </tr>
    </table>
  </xsl:template>
</xsl:stylesheet>
```

nach dem Parsing verworfen. Nachdem diese Voraussetzungen geschaffen sind, kann die eigentliche Arbeit beginnen: die passende Request-Klasse der Shopping-API zu instantiieren und mit den empfangenen CGI-Parametern zu konfigurieren (Listing 2, Abschnitt 3).

Zeitunterschiede bitte beachten

Dafür bekommt der frisch erzeugte Request den externen Suchstring übergeben, dessen vom Client empfangene UTF-8-Kodierung entfernt werden muss, weil der Proxy bei der Generierung des SOAP-Requests alle Parameter ohnehin kodiert. Es folgen die Einschränkungen für die Restlaufzeit der Auktionen von minimal zwei Minuten bis maximal einem Tag. Hier sollte man, wie bei allen Zeitangaben in der Ebay-API, darauf achten, dass die lokale Zeit des Servers nicht zwangsläufig mit der offiziellen Ebay-Zeit übereinstimmt.

Ein NTP-Client sowie am besten zusätzlich eine regelmäßige Bestimmung des Offsets über den API-Call *GeteBayOfficialTime* sind Voraussetzung für zuverlässige Ergebnisse bei zeitkritischen Anwendungen. Die Anfrage wird weiter eingeschränkt: Sie verlangt ein echtes Auktionsformat (im Gegensatz zu Festpreis-, Shop- und anderen), und es dürfen keine Gebote vorliegen. Die Namen der Methoden des Request-Objekts sowie die möglichen Werte der Parameter korrespondieren im Wesentlichen 1:1 mit der XML-Struktur der API.

Außer den Suchkriterien kann und sollte man noch die Sortierung der Ergebnisse festlegen. Für die Schnäppchenjagd heißt das: aufsteigend nach

Listing 4: HTML-Datei

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <script type="text/javascript" src="static/prototype.js"></script>
    <title>Ebay-Suche per Ajax </title>
    <style type="text/css">
      tr.zeile_gerade  { background: #eeeeee; }
      tr.zeile_ungerade {  background: #ffffff; }
      td { padding: 3px; }
      th { background: #dddddd; }
    </style>
  </head>
  <body>
    <p>
      <form onsubmit="findEbayItems($('keywordInput').value); return(false);">
        <input type="text" id="keywordInput" size="15">
        <input type="submit" value="Finden">
      </form>
    </p>
    <div id="ebayItemsContainer">Noch keine Ergebnisse.</div>
  </body>
</html>
```

Endzeit = die in Kürze endenden Auktionen zuerst. Um dem Benutzer die Treffer in verdaulichen Häppchen anbieten zu können, aber nicht selbst große Datenmengen zwischenspeichern zu müssen, nutzt das Skript die API-seitige Paginierung, das heißt es fordert jeweils nur fünf Treffer an, kann aber nach Anforderung des Clients auf beliebige „Seiten“ der so segmentierten Ergebnismenge zugreifen (Listing 2, Abschnitt 4).

Die eigentliche Ausführung des Requests übernimmt der *ServiceProxy*, der als Ergebnis ein Objekt vom Typ *FindItemsAdvancedResponseType* zurückgibt. Vor der Weiterverarbeitung soll er zunächst prüfen, ob das Ergebnis brauchbar ist und nicht etwa ein Kommunikations- oder API-Fehler vorliegt. Falls ja, könnte er es schon fast an den Client weiterreichen, wäre da nicht noch ein kleiner Stolperstein (fehlender Wert, siehe unten), an dem sich die oft auch aus anderen Gründen sinnvolle Anreicherung externer Daten auf dem Feed-Server zeigen lässt: Damit die Navigationselemente für die Ergebnispaginierung bei der XSLT-Transformation des Feeds auf dem Client generiert werden können, müssen die XML-Daten sowohl die aktuelle Seitenzahl als auch die Gesamtzahl der Seiten enthalten. In der API-Response findet sich aber nur Letztere. Die dafür nötige neue Klassenvariable im *FindItemsAdvancedResponseType*-Objekt lässt sich in PHP durch simple Zuweisung festlegen, allerdings muss sie noch das Template mitbekommen, das bei der späteren XML-Serialisierung nötig ist (siehe Listing 2, Abschnitt 5).

Jetzt kann das so ergänzte Response-Objekt wieder in XML gewandelt werden, was ein wenig umständlich, dafür aber flexibel ist; unter anderem können der Name des Root Node gewählt und beliebige On-the-fly-Konvertierungen der Werte definiert werden. Der hier verwendete, mitgelieferte *DataConverterIso* (siehe Listing 2, Abschnitt 6) erledigt beispielsweise die Konvertierung von Zeitangaben zwischen der lokalen Zeitzone und Ebay (GMT).

Transformation nach HTML

Mit dem fertigen Feed ist ein wichtiger Schritt geschafft, allerdings fehlt zu den XML-Daten noch das Stylesheet, das sie im Browser zu HTML transformiert. Der Beispielcode (Listing 3) erzeugt am Root Node einen HTML-Tabellenkopf samt Spaltenüberschriften, und iteriert anschließend über die Kinder des *ebaySearchResults/SearchResult/ItemArray*-Knotens vom Typ *SimpleItem*, die die einzelnen Auktionen repräsentieren. Neben einer alternierenden Vergabe der CSS-Klassen der Tabellenzeilen für bessere Lesbarkeit sind hier die Einbindung eines festen Dummy-Image für Auktionen ohne Galeriebild und die bedingte Erzeugung der „Vor“ und „Zurück“-Verweise der Paginierung im Tabellenfuß interessant. Hier taucht auch der eben eingeschmuggelte *CurrentPage*-Knoten wieder auf, dessen Wert mit dem aus der API stammenden *TotalPages* verglichen wird.

Listing 5: Suchfunktion

```
function findEbayItems(searchString, pageNo) {
var XSLTProc;
var XMLProc;

  var haveXML = false;
  var haveXSLT = false;
  var XMLBuffer;
  function fetchXSLTData() {
    new Ajax.Request
    (
      'styles/ebaySearchResults.xsl',
      {
        onComplete: function(response)
        {
          handleResponse(response, 'XSLTData');
        },
        method: 'get',
        asynchronous: true
      }
    );
  }
  function fetchXMLData() {
    new Ajax.Request
    (
      'feed.php?',
      {
        onComplete: function(response)
        {
          handleResponse(response, 'XMLData');
        },
        method: 'get',
        asynchronous: true,
        parameters: 'page=' + pageNo + '&query='
          + encodeURIComponent(searchString)
      }
    );
  }
```

Weil die Inhalte per Ajax dynamisch eingefügt werden, muss der Content der Seite nur einen minimalen Aufhänger enthalten, der aus dem Suchformular und einem Container für die Ergebnisse besteht, für deren spätere Formatierung noch ein minimalistischer Style vorgesehen ist (siehe Listing 4).

An das Submit-Event des Suchformulars ist ein Aufruf der Funktion *findEbayItems()* gebunden, wobei Prototype die praktische Notation *$('keyword Input')* für das Input-Element ermöglicht.

Den Ergebniscontainer füllen

Was jetzt noch fehlt, ist genau diese Funktion, die den Feed aufrufen, das Stylesheet beschaffen und anwenden sowie schließlich den *ebayItemsContainer* mit dem Ergebnis füllen soll. Zur besseren Übersicht und um die einzelnen Verarbeitungsschritte über asynchrone Callbacks anstoßen zu können, wenn ihre Ausgangsdaten vorliegen, werden im lokalen Scope der Funktion separate Helper zur Beschaffung der XML- und XSLT-Daten und zum Handling der Ergebnisse definiert; Statusvariablen verfolgen den Eingang der Daten.

fetchXSLTData() und *fetchXMLData()* in Listing 5 stützen sich beide auf die bequeme *Ajax.Request*-Klasse von Prototype, deren Konstruktor in einem Aufruf alle nötigen Parameter entgegennimmt, die Callbacks registriert und den REST-Call zur Quelle anstößt, in diesem Fall zum statischen Stylesheet und zum Feed.

Die *handleResponse()*-Funktion behandelt die eingehenden Daten beider Art. Wegen der unterschiedlichen XSLT-Implementierungen im Internet Explorer einerseits und den Gecko-basierten Browsern und Opera auf der anderen sind hier Browser-Weichen erforderlich. Wenn das Stylesheet eintrifft, werden in beiden Fällen der jeweilige XSLT-Prozessor erzeugt und das Stylesheet eingelesen. Beim Eingang der XML-Daten zeigt sich ebenfalls ein Unterschied: Der IE kann das XML in einem *DOMDocument*-Objekt zwischenlagern, während man den anderen Browsern hier mit einem explizit angelegten Puffer unter die Arme greifen muss. Sobald der zweite Callback einschlägt, das heißt alle Daten für die Transformation vorliegen, kann das

Listing 6: Response Handling

```
function handleResponse(response, type)
{
  switch (type)
  {
    case 'XSLTData':
      if (response.status == 200)
      {
        if
        (
          document.implementation
            && document.implementation.createDocument
        )
        {
          XSLTProc = new XSLTProcessor();
          XSLTProc.importStylesheet(response.responseXML);
        }
        else if (window.ActiveXObject)
        {
          XSLTProc = new ActiveXObject('MSXML2.DOMDocument');
          XSLTProc.loadXML(response.responseText);
        }
        haveXSLT = true;
      }
      break;
    case 'XMLData':
      if (response.status == 200)
      {
        if
        (
          document.implementation
            && document.implementation.createDocument
        )
        {
          XMLBuffer = response.responseXML;
        }
        else if (window.ActiveXObject)
        {
          XMLProc = new ActiveXObject('MSXML2.DOMDocument');
          XMLProc.loadXML(response.responseText);
        }
        haveXML = true;
      }
      break;
  }
  if (haveXML && haveXSLT)
  {
    if
    (
      document.implementation
        && document.implementation.createDocument
    )
    {
      $('ebayItemsContainer').update
      (
        getOuterHTML
        (
          XSLTProc.transformToFragment(XMLBuffer, document)
        )
      );
    }
    else if (window.ActiveXObject)
    {
      $('ebayItemsContainer').update
      (
        XMLProc.transformNode(XSLTProc)
      );
    }
  }
}
```

Listing 7: Ende des Javascript-Codes

```
var currentSearchString;
var currentPageNo;
if (!pageNo) pageNo = 1;
else if (pageNo == 'previous') pageNo = currentPageNo - 1;
else if (pageNo == 'next') pageNo = currentPageNo + 1;
currentPageNo = pageNo;
if (!searchString) searchString = currentSearchString;
currentSearchString = searchString;
fetchXSLTData();
fetchXMLData();
```

Rendering nach HTML erfolgen. Hier gibt es ebenfalls leichte Unterschiede: In Gecko-Browsern und Opera muss der DOM-Baum, den der XSLT-Prozessor zurückliefert, explizit in HTML-Quellcode serialisiert werden, während IE dies automatisch erledigt. Das HTML wird direkt aus dem Renderer in die *update*-Methode des Protype-Node-Objekts gespeist, und – endlich – bekommt der Benutzer das Ergebnis zu sehen.

Ironischerweise kennt IE ein natives *outerHTML*-Property für alle DOM-Elemente, obwohl es dort in diesem Kontext nicht nötig ist, während die Serialisierung für Gecko-Browser und Opera hergestellt werden muss:

```
var xmlserializer;
function getOuterHTML(element) {
  if (!xmlserializer) {
    xmlserializer = new XMLSerializer();
  }
  return xmlserializer.serializeToString(element);
}
```

Am Fuß der *findEbayItems()*-Funktion in Listing 5 ist noch über den aktuellen Stand von Suchbegriff und Page Buch zu führen, damit die relativen Calls aus den Paginator-Links bedient werden können, und schließlich sind *fetchXSLTData()* und *fetchXMLData()* anzustoßen, um den ganzen Mechanismus in Gang zu bringen (siehe Listing 7).

Fazit

Um hier nicht nur isolierte Codefragmente, sondern ein in sich geschlossenes, lauffähiges Codebeispiel zeigen zu können, mussten alle Extras außen vor bleiben, vor allem ein schickes Aussehen. Der Tauglichkeit der beschriebenen Techniken für den professionellen Einsatz tut das aber keinen Abbruch, und so bleibt zu hoffen, dass jeder, der bis hierhin gelesen hat, eigene Ideen für kreative Ebay-Anwendungen im Kopf hat. (hb)

ANDREAS OESTERHELT

ist einer der Köpfe hinter InTradeSys. Das Kölner Softwarehaus entwickelt E-Commerce-Lösungen für Online-Marktplätze und deren Kunden. Im Auftrag von Ebay sind dabei das PHP-SDK für die Ebay-API sowie zahlreiche weitere Projekte entstanden.

JAN SEIDLER

ist bei Ebay Deutschland für Produkt-Strategie und -Innovation zuständig. Er leitet das Team, das sich mit der Planung und Entwicklung von Prototypen und nicht zuletzt mit dem Ebay Developers Program beschäftigt.



Facebook-Applikationen entwickeln

Das eigene Gesicht

Ramon Wartala

Nicht nur, dass das Studentennetz Facebook einen riesigen Erfolg hatte – über eine API kann jeder Anwendungen schreiben, die dort integrierbar sind.

Als der 24-jährige Facebook-CEO Mark Zuckerberg am 24. Mai 2007 seine Rede zur Öffnung der Facebook-Plattform hielt (siehe Onlinequellen [d]), ging ein Rauschen durch den Blätterwald. Google Trends vermerkte für diesen Tag einen steilen Anstieg des Interesses an Facebook. Aus Marketing- wie technischer Sicht kann diese Ankündigung sicherlich als Coup gelten. Facebook öffnete sein soziales Netz für Fremdanwendungen. Dabei lässt das Studentenportal Entwickler nicht nur auf die eigene Datenbasis zugreifen, sondern ermöglicht außerdem die visuelle Einbindung persönlicher Inhalte und die Verteilung der Applikation über die Facebook-Plattform selber.

Im Klartext heißt das: Potenziell kann man mit einer Applikation mehr als 60 Millionen Nutzer erreichen, Tendenz steigend. Und das wiederum bringt für Facebook entscheidende Vorteile. Durch das als Crowdsourcing bezeichnete Nutzen fremder und für Facebook kostenloser Entwicklungsressourcen gewinnt das Netz jede Menge Anwendungen hinzu, und Anwendungsfälle gibt es reichlich: Spiele, E-Mail-Anbindung, To-do-Listen, Kalender und ganze Office-Applikationen wie die Einbindung von Zoho [a] zeigen, dass großes Interesse an Facebook als Integrationsplattform besteht.

Etablierte Anwendungen erreichen mit ihrer Ausprägung in Facebook auf einen Schlag eine höhere Nutzerschaft, neue Anwendungen, die ganz auf den sogenannten Social Graph [b] setzen, ermöglichen sogar kleinen Firmen mit innovativen Ideen einen schnellen Markteintritt.

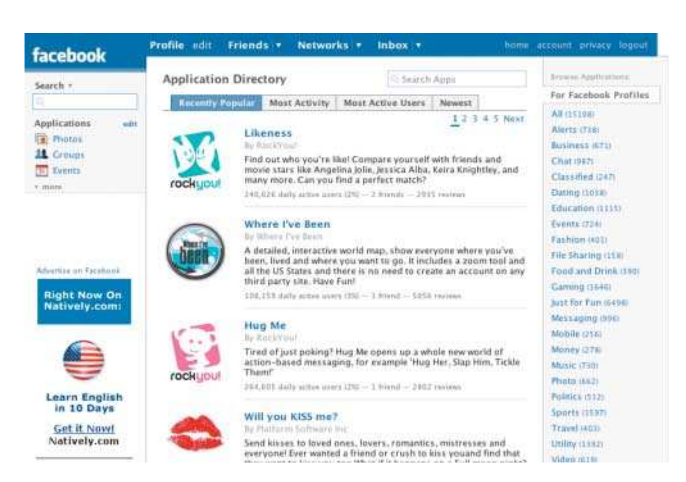
Um zu verstehen, was eine Facebook-Applikation kann und darf, muss man den Aufbau und die Anknüpfungspunkte kennen, an der man die eigene Applikation in die Plattform „einhaken“ kann. Kern eines jeden sozialen Netzes sind Beziehungen zu Freunden und Bekannten. In Facebook können Nutzer diese leicht über die integrierte Such- und Einladefunktion aufbauen. Sind genug Beziehungen geknüpft, kann jeder innerhalb des Freundesnetzes die Aktionen anderer über sogenannte „Status Updates“ verfolgen. Bei jedem Upload von Fotos, Videos oder dem Editieren von Notizen erhält der Freundeskreis eine Nachricht. Und das nutzen externe Anwendungen wie Twitter und del.icio.us, um über Änderungen ihrer Datenbasis Auskunft zu geben. Sucht man den direkten Kontakt, kann man über das interne Mailsystem oder über die „Wall“ Nachrichten austauschen. Eine Zusammenfassung aller Aktionen des eigenen Netzes bekommt man über den „News Feed“ angezeigt.

Die Nutzung all dieser Funktionen ist nicht auf das Web beschränkt. Eine Anbindung für Mobiltelefone [e, f] existiert ebenso wie mehrere Desktop-Integrationen. Im Folgenden soll es um eine Facebook-Applikation gehen, die in der Webversion zur Anwendung kommen soll. Zuvor ein kurzer Überblick über die zentralen Bestandteile der Oberfläche.

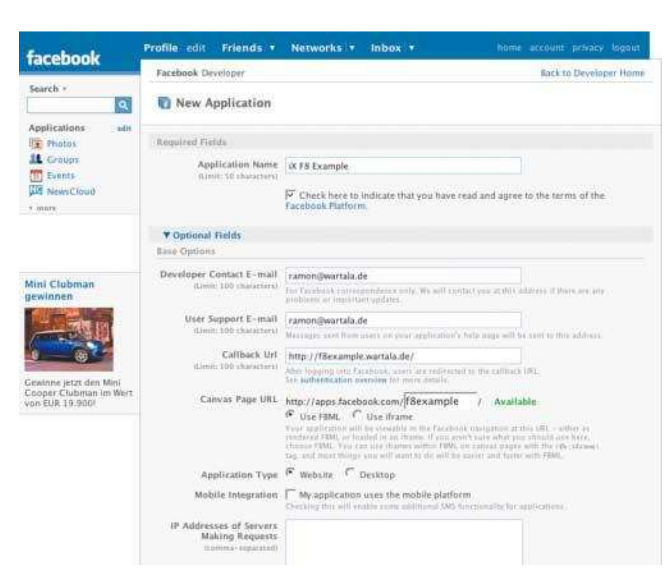
15 000 Anwendungen vorhanden

Facebook bringt von Haus aus einige Anwendungen mit, die sich über die linke Navigationsleiste anwählen lassen. Hier sind alle mit kleinen Icons auswähl- und konfigurierbar. „Applications“ als Menüpunkt führt den Nutzer auf eine Auswahlseite mit allen installierten Anwendungen im eigenen Profil. Über „Browse More Applications“ (siehe Abbildung 1) lassen sich weitere Anwendung zum eigenen Profil und in die linke Navigation hinzufügen oder löschen. Momentan (Februar 2008) sind über das Applikationsverzeichnis mehr als 15 000 Anwendungen nutzbar.

Die eigentliche Anwendung kann auf ganz unterschiedliche Arten in Facebook präsent sein. Im einfachsten Fall



Facebooks Anwendungsverzeichnis: Rechts kann man sich durch die gesamte Liste „hangeln" (Abb. 1).



Konfiguration der eigenen Facebook-Anwendung – bis hin zur Wahl zwischen FBML und *iframe* (Abb. 2)

präsentiert sie sich als sogenannte „Canvas Page" in der Mitte der Benutzeroberfläche, großflächig. Anwendungen dürfen entweder über einen externen Aufruf innerhalb eines *iframe* zur Darstellung kommen oder ihre Daten via Facebook Markup Language (FBML) zurückliefern. Einen weiteren Anknüpfungspunkt bietet die sogenannte Profilseite, die dem Nutzer als zentraler Ort seiner Onlinepräsenz dient. Eigene Anwendungen sollten nur eine begrenzte Menge ihrer Informationen hier anzeigen. Eine ausführliche Übersicht über die Anatomie einer Facebook-Applikation findet sich unter [g].

Eigener Webspace erforderlich

Entwickler-Applikationen residieren nicht bei Facebook, sondern auf einem aus Facebook-Perspektive entfernten Rechner, der als Callback die nötigen Anwendungsdaten übermittelt. Jede Anwendung ist innerhalb von Facebook über eine eindeutige URL zu erreichen. Über sie wird der Redirect auf die eigene Anwendung ausgeführt. Die gibt nun ihrerseits Facebook-konformen Code in die Oberfläche zurück. Das führt dazu, dass sich Facebook im Ganzen etwas langsamer „anfühlt" als klassische Webanwendungen.

Entwicklern einer Facebook-Applikation stehen eine ganze Reihe von Techniken zur Verfügung:
– API: stellt Methodenaufrufe über eine REST-Webservice-Schnittstelle zur Verfügung,
– Markup Language (FBML): erlaubt den Zugriff auf alle Teile der Facebook-Oberfläche,
– Query Language (FQL): für den Zugriff auf die Informationsbestandteile über eine SQL-ähnliche Anfragesprache,
– Javascript (FBJS): Script-Einbindung in die eigene Anwendung.
Die folgenden Codebeispiele sollen sich nur auf einen kleinen Teil der API und der FBML konzentrieren.

Klassisch beginnen Einführungen in Programmiersprachen oder Frameworks mit „Hello World". Es stellt die denkbar simpelste Funktion dar, die eine Anwendung ausführen kann. Um eine ebenso einfache Anwendung für Facebook aufzusetzen, ist das folgende, schrittweise Vorgehen nötig. Doch bevor es so richtig losgehen kann, ist ein eigenes Profil erforderlich. Dieses lässt sich von der Homepage aus mit wenigen Angaben einrichten.

Am Anfang jeder Facebook-Applikation steht die Seite developers.face book.com/get_started.php, die einen leeren Anwendungs-Container als Startpunkt in das eigene Profil einfügt. Über „Set Up New Application" lässt sich die erste eigene Anwendung über einen maximal 50 Zeichen langen Namen konfigurieren. Ist der festgelegt, sollte man die Platform Terms bestätigen und die optionale Parameteransicht aufklappen und bearbeiten.

Außer der Entwickler- und Nutzer-E-Mail-Adresse, die standardmäßig mit der eigenen vorbelegt ist, muss man die Callback-URL angeben. Schon an diesem Punkt sollte man sich Gedanken über das Hosting der eigenen Applikation machen. Eigene Facebook-Anwendungen setzen zwingend eine eigene Webpräsenz voraus. Die genauen Anforderungen zum Betrieb beschreibt der Kasten „Voraussetzung für den Anwendungsbetrieb".

Nach dem Eintragen aller Formulardaten (zuzüglich „Submit") bekommt man den nötigen API-Schlüssel und das zugehörige Passwort angezeigt, mit denen sich die eigenen Anwendung bei Facebook authentifizieren muss.

Spätestens an dieser Stelle stellt sich die Frage nach der Programmiersprache, in der die eigene Anwendung geschrieben sein soll. Facebook bietet offiziell nur Client-Bibliotheken für PHP4, PHP5 sowie für Java an. Im Developer Wiki [h] gibt es jedoch eine breite Unterstützung für viele gängige Programmiersprachen und Webframeworks. Leider ist an dieser Stelle nicht immer Verlass auf die Aktualität der Wiki-Einträge. So findet sich unter der

iX-TRACT

- Im Mai 2007 hat Facebook sein soziales Netz für Anwendungen geöffnet.
- Die API für den Zugriff auf Facebook arbeitet über REST und erlaubt es, Javascript einzubinden.
- Mit einer eigenen Auszeichnungssprache (FBML) liefert Facebook spezielle Tags für das Anbinden an die Umgebung.



Hinzufügen der selbsterstellten Anwendung zum eigenen Facebook-Profil (Abb. 3)

Voraussetzung für den Anwendungsbetrieb

Ein einfaches Webhosting-Paket der gängigen Anbieter reicht für die ersten Experimente mit der Facebook-Anwendungsschnittstelle aus. Konkret ist ein Webserver erforderlich, der mindestens PHP4-Skripte ausführen können sollte. Installieren lässt sich die Facebook-API mit

```
wget http://developers.facebook.com/clientlibs/↵
                                facebook-platform.tar.gz
tar -xvzf facebook-platform.tar.gz
```

Auf Systemen ohne *SimpleXML*-Bibliothek kann man diese einfach über

```
wget http://downloads.sourceforge.net/↵
        ister4framework/simplexml44-0_4_4.tar.gz
tar -xvzf simplexml44-0_4_4.tar.gz
```

nachinstallieren. Sind beide Voraussetzungen erfüllt, reicht ein normales, PHP-fähiges Verzeichnis auf dem Webserver aus.

Möchte man die eigene Anwendung der breiten Nutzerschar im Facebook-eigenen Applikationsverzeichnis zur Verfügung stellen, benötigt man mindestens fünf Nutzer, die die eigene Anwendung einsetzen. Was sich als einfache Einstiegshürde erweist, hat in der Praxis ihre Tücken. So kann es vorkommen, dass viele Tausend Nutzer die eigene Anwendung einbinden, den eigenen Webserver und die eventuell limitierte Bandbreite und Traffic über Nacht ins Wanken bringen. Was wiederum die Facebook-Plattform mit Fehlermeldungen bestraft, da sie keine Antwortzeiten von mehreren Sekunden Länge toleriert. Mittlerweile existieren jedoch schon etliche Lösungen von Anbietern, die spezielle Facebook-Hosting-Services übernehmen (beispielsweise joyent.com/developers/facebook).

Rubrik „Ruby on Rails“ immer noch der Eintrag zur Client-Bibliothek RFacebook. Die Weiterführung dieser Bibliothek hat ihr Entwickler Matt Pizzimenti jedoch Mitte Januar 2008 eingestellt. Von Chat Fowlers alternativem Bibliothek Facebooker [i] erfährt der Interessierte erst ganz am Ende der entsprechenden Wiki-Seite.

Ausgangspunkt: Die Klasse *Facebook*

Im Folgenden soll die offizielle PHP-Bibliothek von Facebook zum Einsatz kommen, da sich damit die ersten Gehversuche einfach gestalten. Ausgangspunkt der PHP-Bibliothek ist die Klasse *Facebook*, die den Zugang und die nötigen API-Aufrufe kapselt und an die API weiterleitet (siehe Listing 1).

Zeile 6 generiert eine Instanz der Wrapper-Klasse *Facebook*. Zeile 15 gibt die Begrüßung an den Benutzer aus. Der Tag *<fb:name>* ist Bestandteil von Facebooks Markup Language.

Listing 1: Hello World

```
1  <?php
2  /* Facebook Client-Bibliothek einbinden */
3  require_once('facebook.php');
4
5  /* Facebook-API mit Anwendungs-Schluessel und -Passwort initialisieren */
6  $facebook = new Facebook('XXXXXXXXXXXXXX','XXXXXXXXXXXXXX');
7
7  /* Ein eingeloggter Benutzer ist noetig, bevor die Anwendung genutzt
8     werden kann. Ist der Benutzer nicht eingeloggt, wird ihm
10    eine Login-Aufforderung praesentiert
11 */
12 $fb_user = $facebook->require_login();
13 ?>
14
15 Hallo iX-Leser <fb:name uid='<?php echo $fb_user; ?>'
16 useyou='false' possessive='true' /> und herzlich willkommen bei
17 Ihrer ersten Facebook-Applikation!
```

Echtes HTML ist an dieser Stelle nur eingeschränkt möglich. Ist diese „Hello World“-Anwendung im Internet erreichbar, ruft der Webbrowser des Nutzers sie durch die eigentliche Facebook-Umgebung über die Callback-URL auf, die an die Facebook-Oberfläche das zugehörige FBML zurückliefert.

Zum Prüfen der Anwendung kann entweder die Callback-URL oder die registrierte Facebook-URL dienen. Vergleicht man die zurückgegebenen Informationen, wird schnell klar, was FBML im Kern tut. Die Tags werden gefiltert, ausgewertet und mit Daten und Styling versehen. Einen Überblick über alle FBML-TAGs findet sich im Entwickler-Wiki [j]. Grob lassen sich die Tags in folgende Gruppen sortieren:

- Social Data Tags: Anzeige und Formatierung von Informationen im sozialen Netz,
- Sanitization Tags: Einbindung externer Browser-Objekte wie Flash, Silverlight oder einfache MP3-Dateien,
- Design Tags: Anpassung des Aussehens der eigenen Anwendung im Facebook-Styling,
- Komponenten-Tags: Einsatz bekannter Facebook-Muster in eigenen Anwendungen wie die Kommentarfunktion,
- Kontroll-Tags: Kontrolle über bestimmte Informationen.

Listing 2: Liste aller Freunde mit Bildern

```
1 $fb_friends = $facebook->api_client->friends_get();
2 echo "<div style='padding: 10px;'>\n";
3 echo "<h1>Liste meiner Freunde:</h1>\n";
4 foreach ($fb_friends as $friend) {
5     $photo = $facebook->api_client->users_getInfo($friend, 'pic');
6     echo "<img src='".$photo[0]['pic']."' />";
7     echo "<fb:name uid='".$friend."' /> <br />\n";
8 }
9 echo "</div>\n";
```

Damit sich Informationen per FBML darstellen lassen, müssen Anwendungen diese über die Facebook-API abfragen. Dazu stehen eine Reihe von Methoden zur Verfügung [k]. Listing 1 enthielt schon die API-Funktion *require_login()*. Dass Facebook darüber hinaus mächtigere Aufrufe parat hält, demonstriert Listing 2. Über die *friends.get*-Funktion kann man ein Array des gesamten eigenen Freundeskreises erstellen.

Zeile 1 ruft die API-Funktion auf und liefert eine Liste der Nutzer-IDs (UID) zurück. Über diese UID lassen sich eine Menge Informationen abrufen. Exemplarisch sei in Zeile 5 die API-Funktion *users.getInfo* mit der UID aufgerufen, die in diesem Fall das Bild der Freundin oder des Freundes als Image-URL liefert und mit dem Namen als Liste ausgeben kann.

Ganz im Sinne der Remix- und Mashup-Kultur lassen sich externe Quellen ebenfalls anzapfen und in der eigenen Facebook-Anwendung darstellen. Listing 3 bindet die freie MagpieRSS-Bibliothek [c] ein, um einen Atom-Newsfeed abzurufen und darzustellen.

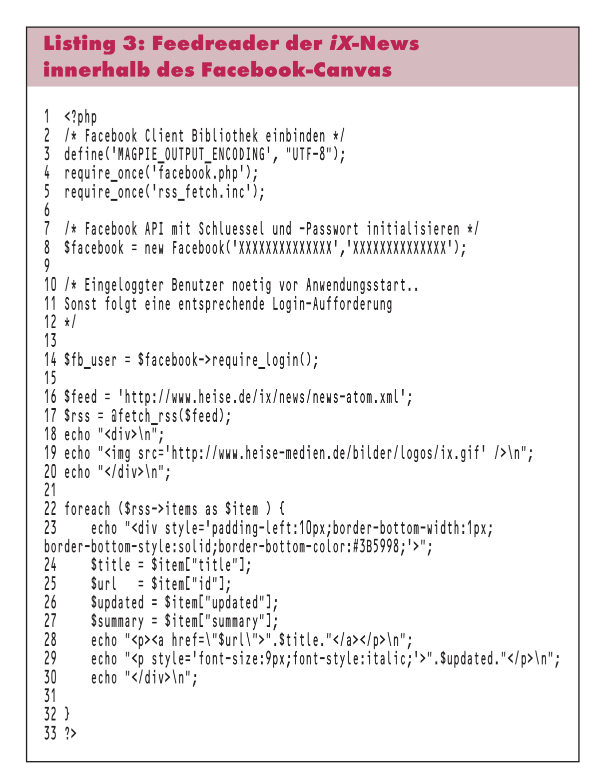
Zeile 17 holt den Atom-Feed und baut in den folgenden Zeilen das Layout für die einzelnen Nachrichten auf. Bei diesem Codebeispiel sind CSS-Attribute für das Aussehen der Informationen eingebettet.

Nach den ersten Schritt stellt sich schnell die Frage nach einem Styleguide für Facebook. In den offiziellen FAQ [14] findet sich dazu ein minimaler Abschnitt, der Farbcodes für Überschriften, Hintergrundfarben, Boxen und Linien aufführt und Größenbeschränkungen der einzelnen Anwendungspunkte beschreibt. Offizielle Werkzeuge [m], mit denen man API-Aufrufe und FBML-Tags testen kann, sollen das Leben des Facebook-Entwicklers vereinfachen.

Für wen Facebook wertvoll ist

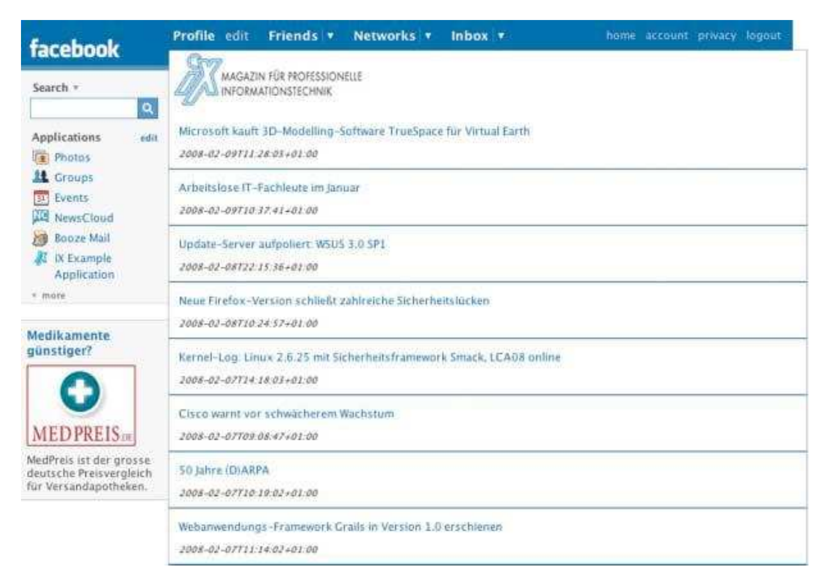
Jenseits der immer absurderen Schätzungen über den wahren Wert von Facebook stellt sich die Frage, warum über 60 Millionen aktiver Nutzer weltweit auf dieser Plattform über 15 000 3rd-Party-Anwendungen nutzen.

Drei Nutzergruppen lassen sich auf Facebook identifizieren: als erste die der reinen Anwender, die über Facebook ihre Freundschaften pflegen, Fotos hochladen, Notizen online stellen und sich über den Status der



Listing 3: Feedreader der *iX*-News innerhalb des Facebook-Canvas

```
1  <?php
2  /* Facebook Client Bibliothek einbinden */
3  define('MAGPIE_OUTPUT_ENCODING', "UTF-8");
4  require_once('facebook.php');
5  require_once('rss_fetch.inc');
6
7  /* Facebook API mit Schluessel und -Passwort initialisieren */
8  $facebook = new Facebook('XXXXXXXXXXXXXX','XXXXXXXXXXXXXX');
9
10 /* Eingeloggter Benutzer noetig vor Anwendungsstart..
11 Sonst folgt eine entsprechende Login-Aufforderung
12 */
13
14 $fb_user = $facebook->require_login();
15
16 $feed = 'http://www.heise.de/ix/news/news-atom.xml';
17 $rss = @fetch_rss($feed);
18 echo "<div>\n";
19 echo "<img src='http://www.heise-medien.de/bilder/logos/ix.gif' />\n";
20 echo "</div>\n";
21
22 foreach ($rss->items as $item ) {
23     echo "<div style='padding-left:10px;border-bottom-width:1px;
border-bottom-style:solid;border-bottom-color:#3B5998;'>";
24     $title = $item["title"];
25     $url   = $item["id"];
26     $updated = $item["updated"];
27     $summary = $item["summary"];
28     echo "<p><a href=\"$url\">".$title."</a></p>\n";
29     echo "<p style='font-size:9px;font-style:italic;'>".$updated."</p>\n";
30     echo "</div>\n";
31
32 }
33 ?>
```



Der *iX*-Newsfeed findet sich innerhalb von Facebook links im Menü – und hier rechts nach dem Klick (Abb. 4).

eigenen Kontakte informieren. Zum anderen der Betreiber der Plattform selber, dessen Wert sich logischerweise an den Nutzerzahlen orientiert. Nicht zuletzt, weil Facebook einen Teil der Seiten mit klassischer Onlinewerbung versehen hat.

Um der Werbewirtschaft die Ansprache relevanter Zielgruppen auf einfache Weise zu ermöglichen, kündigte Facebook im November letzten Jahres das sogenannte Targeting (die gezielte Auslieferung von Onlinewerbung) auf die Profile der Nutzer an. Schaut man sich diese heiß (www.spiegel.de/netzwelt/web/0,1518,druck-519295,00.html) diskutierten Möglichkeiten etwas genauer an (blog.nugg.ad/de/2007-11-10/facebook-targeting-womit-eigentlich/), bleibt nicht viel mehr als das Auffinden von Altersklassen und dem Geschlecht der Nutzer, deren Angabe aber beliebig falsch sein kann.

Als dritte Gruppe verfolgt eine große Zahl von 3rd-Party-Entwicklern wenigstens zwei Ziele auf Facebook:

1. Ihr eigenes Angebot bekanntmachen, um möglichst viele Nutzer bei Facebook „abzuholen“. Steuert der Nutzer den 3rd-Party-Dienst an, kann dieser seine Leistungen monetarisieren lassen.

2. Anwendungen für Werbekunden wie Spiele (Advergames) erstellen, die die Marke des Werbenden und seine Bekanntheit steigern.

Facebook selber ist in der schwierigen Position, alle Nutzergruppen berücksichtigen zu müssen. An Neuerungen wie der Beacon-Funktion für gezielte Werbung (en.wikipedia.org/wiki/Beacon_%28Facebook%29) wurde in der Vergangenheit allerdings ersichtlich, wie schwierig sich neue Vermarktungsansätze etablieren lassen. Je mehr Nutzer es sind und je länger sie Facebook als virtuellen Aufenthaltsort nutzen, desto mehr interessiert sich die Werbewirtschaft für diesen Standort.

Fazit

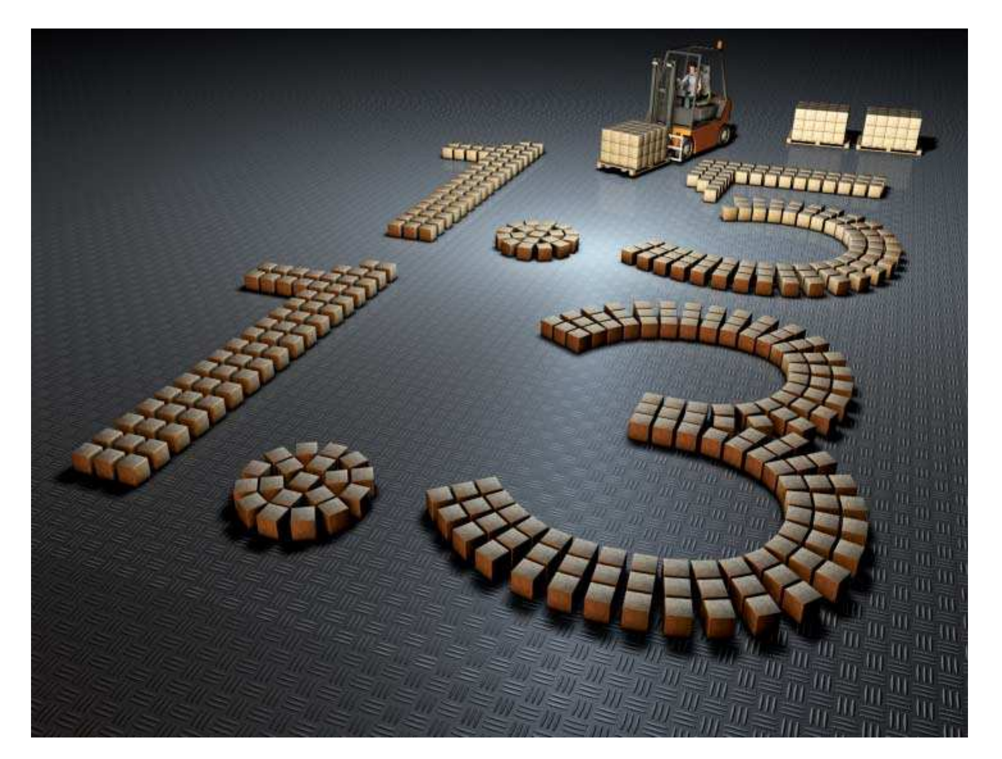
Die Nutzer- und Anwendungszahlen auf Facebook sprechen eine deutliche Sprache. Es ist der Firma ganz offensichtlich gelungen, eine Plattform für ihre Nutzer und für externe Entwickler attraktiv zu gestalten. Für Website-Betreiber ist alleine die Anzahl potenzieller Nutzer so interessant, dass einige sicherlich die damit verbundenen Risiken (siehe Kasten) auf sich nehmen werden. Bleibt für Entwickler nur zu hoffen, dass Werkzeuge nicht allzu lange auf sich warten lassen, die es ermöglichen, Anwendungen für beide APIs zu erstellen. (hb)

RAMON WARTALA

ist IT-Leiter beim Hamburger Onlinevermarkter orangemedia.de GmbH. Er ist Koautor des Buches „Webanwendungen mit Ruby on Rails“, das 2007 bei Addison-Wesley erschienen ist.

Onlinequellen

Diverses	
[a] Office-Anwendungen mit Zoho	www.facebook.com/apps/application.php?id=2380274266
[b] Konzept des Social Graph	www.readwriteweb.com/archives/social_graph_concepts_and_issues.php
[c] MagpieRSS-Bibliothek für PHP	magpierss.sourceforge.net/
Facebook-Links	
[d] Mark Zuckerbergs „Öffnungs“rede	developers.facebook.com/videos.php?f8_keynote
[e] für Mobiltelefone	m.facebook.com/
[f] für das iPhone	iphone.facebook.com
[g] Anatomie	developers.facebook.com/anatomy.php
[h] Development Wiki	wiki.developers.facebook.com/index.php/Main_Page
[i] Chat Fowlers Ruby Framework	facebooker.rubyforge.org/
[j] Facebook Markup Language	wiki.developers.facebook.com/index.php/FBML
[k] API	wiki.developers.facebook.com/index.php/API
[l] Developer FAQ	wiki.developers.facebook.com/index.php/FAQ
[m] Developer Tools	developers.facebook.com/tools.php



Subversion 1.5: Mehr als nur der CVS-Nachfolger

Sprung nach vorn

Kai Gellien, Andreas Leibl

Die neue Version 1.5 bereichert das zentralistische Subversion um Features, die man von verteilten Versionsverwaltungen kennt. Im vergangenen Oktober konnten sich die Teilnehmer der Subversion-Konferenz bereits die kommende Release ansehen, nun steht die Alpha-Version zum Download bereit.

Gut zwei Jahre nach der Freigabe von Subversion 1.3 steht Version 1.5 ins Haus. Mit der offiziellen Freigabe ist im Laufe des April zu rechnen. Nachdem Version 1.4 eher unspektakulär war und sich mehr der Produktpflege widmete, ist die 1.5er-Ausgabe wieder eine sogenannte Feature-Release. Nach Angaben der 1999 gegründeten Firma Collabnet, Hauptsponsor des Open-Source-Projekts, handelt es sich um die größte Release seit der Version 1.0 [1].

Natürlich verfolgt Collabnet auch kommerzielle Interessen. Zum einen bietet die Firma Dienstleistungen rund um die freie Version von Subversion an und hat daneben eigene Software für kommerzielle Nutzer im Angebot, die auf der freien Version basiert. Zur eigenen Collabnet Enterprise Edition kauften die Kalifornier im vergangen Jahr die Sourceforge Enterprise Edition, die kommerzielle Ausgabe der beliebten Open-Source-Plattform, von VA Software hinzu.

Subversion (SVN) hat man mit dem erklärten Ziel entwickelt, ein „besseres“ CVS (Concurrent Versions System) zu implementieren. Wichtig war, ein ähnliches Look & Feel zu bewahren, um der großen Gemeinde der CVS-Nutzer den Umstieg zu erleichtern. Verbessert wurden zuerst die Stellen, an denen CVS die größten Defizite aufwies, beispielsweise Branching und Tagging sowie die Verwaltung von Verzeichnissen. Beim Merging, also dem Kopieren von Änderungen zwischen Entwicklungszweigen, mag Subversion zwar besser sein als CVS. Verteilten Versionsverwaltungssystemen war es in diesem Bereich jedoch unterlegen. Diese haben aufgrund ihrer Architektur, sozusagen von Natur aus, die Nase vorn. Kommerzielle Systeme wie Clearcase bieten in diesem Bereich ebenfalls mehr. Insbesondere Enterprise-Kunden, die migrieren, möchten auf solche Features, an die sie gewöhnt sind, nicht verzichten. Diese Lücke soll Subversion nun schließen.

Dies ist insofern notwendig, als Subversion zwar weiter starken Zulauf erfährt – Anfang Februar gab es über 220 000 öffentliche Apache-Server, die per WebDAV Zugang zu Subversion-Repositories boten –, aber dennoch schon einige wenige, aber prestigeträchtige Projekte an verteilte Versionsverwaltungssysteme verloren hat. So hat sich etwa das Mozilla-Team dafür entschieden, sein in die Jahre gekommenes CVS eben nicht durch den etablierten Nachfolger, sondern durch Mercurial(Hg) zu ersetzen.

Transaktionen replizieren und kompakter speichern

Mit *svnsync* lässt sich ein (Master-)Repository in eine (beliebige) Anzahl von Read-Only-Kopien replizieren. Nützlich ist *svnsync* etwa für Back-Up-Zwecke oder – bei (international) verteilter Entwicklung – um auch bei Netzausfall ein Repository zum Auschecken für den Build zur Verfügung zu haben. In der Regel sind Lesezugriffe auf das Repository häufiger als Schreibzugriffe, sodass *svnsync* außerdem der Lastverteilung dienen kann.

Bemerkenswert ist, dass alle drei Beteiligten, Quell- und Ziel-Repository sowie *svnsync* selbst, auf verschiedenen Computern laufen können, da *snvsync* über die Subversion-API Transaktionen ausliest und wieder einspielt, statt einfach nur Daten zu kopieren. Letzteres könnte auch ein Programm wie *rsync*, der Transaktionsansatz ist aber robuster, vor allem bei nicht allzu verlässlichen Netzverbindungen.

Da man typischerweise aus einem Repository nicht nur lesen, sondern auch

hineinschreiben möchte, kommt der neue WebDAV Write Through Proxy gerade recht. Er ermöglicht es Entwicklern, die Apache-gestützte Repositories betreiben, (am replizierten Repository vorbei) direkt in das Master-Repository zurückzuschreiben, um diese Änderung anschließend zurückzureplizieren. Die Realisierung dieses Features in *svnserve* wäre – so die Auskunft der Entwickler – zu aufwendig gewesen. Da bei den meisten Systemen, für die ein Write Through interessant ist, sowieso der besser skalierende Apache installiert ist, hat man auf einen *svnserve* Write Through Proxy vorläufig verzichtet.

Für ein kompakteres Repository sorgen die Verbesserung des binären Delta-Algorithmus und die komprimierte Speicherung der „delta-chunks“. Um für bestehende Repositories in den Genuss der neuen Schlankheit zu kommen, müssen die Anwender sie zuerst auf die Platte speichern und anschließend in die mit dem neuen Subversion erzeugten Repositories einspielen.

Im Test wurde dies beispielhaft an einem Repository mit über 1000 Dateien (Sourcecode und Binaries wie Excel) und über 600 Revisions durchgeführt. Die Größe des Repository schrumpfte von gut 13 MByte auf etwa 9 MByte. Damit lag die Platzersparnis in diesem konkreten Fall bei circa 30 Prozent.

Verwalten jenseits von CVS

Windows-Anwender nehmen sicherlich dankbar zur Kenntnis, dass *svnserve* nun als Windows Service zur Verfügung steht. Dadurch spart man sich einige Klimmzüge bei der Einrichtung eines Subversion-Servers.

Spätestens mit der in einem früheren *iX*-Artikel [2] besprochenen Version 1.3 haben die Entwickler ihr Ziel – die Ablösung von CVS – erreicht. Das zeigen auch Nutzungsstatistiken von Collabnet. Subversion ist plattformübergreifend wie der Vorgänger und hat einen vergleichbaren Funktionsumfang, der zudem um einige Freatures wie WebDAV erweitert wurde. Das alles sowie eine an CVS angelehnte Bedienung machten den Umstieg leicht. Die breite Tool-Unterstützung und die Aufnahme in IDEs wie Eclipse taten ein Übriges.

Doch nur ein besseres CVS zu bieten, genügte den SVN-Entwicklern auf die Dauer nicht. Deshalb veranstaltete Collabnet – Arbeitgeber einiger der Kernentwickler – Anfang 2006 ein Treffen mit Firmenkunden, um deren Hauptanforderungen herauszuarbeiten.

Im Gegensatz zu vielen Open-Source-Projekten haben diese Kunden oft viele, teilweise langlebige Branches, beispielsweise für aufeinanderfolgende Versionen ihrer Software. Ältere Releases bleiben oft über Jahre in der Wartung, und Patches für Fehler oder Sicherheitsprobleme muss man für mehrere Ausgaben portieren. Von Zeit zu Zeit werden auch neue Features in ältere Releases rückportiert, sodass die Programmierer Entwicklungszweige regelmäßig abgleichen müssen. Davon sind häufig viele Dateien betroffen.

Merge Tracking erfüllt Wünsche

Wenn die Versionsverwaltung keine Unterstützung für das Tracking dieser Merge-Vorgänge bietet, bleibt einem Entwicklerteam nur die Option, selbst genau Buch darüber zu führen. Denn weder will man eine Änderung unabsichtlich auslassen, noch einen Merge doppelt ausführen. Unter Umständen ist auch die Beweisbarkeit von Modifikationen („Audit Trail“), von Bedeutung. Deshalb stand Merge-Tracking ganz oben auf der Wunschliste der (zahlenden) Kunden.

Bevor Merge Tracking in Subversion aufgenommen wurde, bot ein Python-Skript externe Unterstützung. Dies war gleichzeitig ein Test für das Konzept, solche Merges über Properties zu protokollieren. Merge Tracking in Subversion 1.5 entspricht im Wesentlichen der Funktion dieses Skripts, ist aber feingranularer und ermöglicht es, nur eine Auswahl von Änderungen zu übernehmen (Cherry Picking).

Die Merge History dient unter anderem dazu, doppelte Merges zu vermeiden. Kollidieren die Änderungen eines Entwicklungszweiges mit denen im Ziel-Branch, erkennt der Subversion-Client dies, bevor ein Commit die Änderungen zurückschreibt. Der Benutzer kann in einem solchen Fall das Problem interaktiv lösen. Je nach Umgebung geschieht das in einem GUI-Tool (etwa mit Collabnets GUI Merge Client) oder auf der Kommandozeile.

Die bisher implementierten Features sind aber erst der Anfang. Für Nachfolgeversionen haben die Entwickler weitere Funktionen geplant, unter anderem „blocking of changes“, diverse Auditing- beziehungsweise Reporting-Funktionen sowie die Behandlung zyklischer Merges.

Oft arbeiten Entwickler an mehreren Tasks gleichzeitig. Change Lists erlauben es, die bearbeiteten Dateien unter einem Namen zusammenzufassen und auf diese Liste Operationen wie Commits

Wichtige neue Features in Subversion

Neu in SVN 1.4

– kompakteres Repository-Format spart Plattenplatz

– *svnserve* nun auch als Windows Service

– *synsync* erlaubt sicheres Spiegeln von Repositories

Neu in SVN 1.5

– WebDAV Write Through Proxy

– Merge Tracking vereinfacht die Verwaltung mehrerer Entwicklungslinien

– Change Sets und Cherry Picking unterstützen bei der Portierung von Patches

– Sparse Directory Support ermöglicht ein fein granulareres Auschecken von Teilen eines Projekts

oder Vergleiche zu anderen Versionen durchzuführen. *svn status* listet die Zugehörigkeit zu Change Lists optisch gut getrennt auf.

Die Zugehörigkeit zu einer Changelist wird aber nur lokal gespeichert und anders als andere Dateiattribute nicht im Repository abgelegt. Auch geht die Information bezüglich der Zugehörigkeit zu einer Change List nach einem Commit verloren. Des Weiteren kann eine Datei nur zu maximal einer Change List gehören.

Dieses Feature wurde stark von den Funktionen inspiriert, die Perforce bietet, und an das deutlich andere Netzwerkmodell von Subversion angepasst.

Checkout auch einzelner Ebenen

Eine andere Möglichkeit, mit Änderungen in Teilprojekten umzugehen, ist ein Checkout lediglich der Teilbäume, an denen man selbst arbeiten will. Ab Version 1.5 geht dies feingranularer dank des neuen Sparse Directory Supports.

Die Arbeiten am Sparse Directory Support – auch als Workspace Management bezeichnet – vertrugen sich nicht gut mit den Arbeiten am Merge Tracking. Die Überschneidung der Codebereiche erschwerten das Debugging und waren mit verantwortlich für die erheblichen Verzögerungen bei der Freigabe der Version 1.5.

Wie schon in den vorherigen Versionen sind sowohl der 1.5er-Client als auch der Server rückwärtskompatibel. Zwar lassen sich nur dann alle Features nutzen, wenn beide Seiten auf dem letzten Stand sind, trotzdem wirft der Betrieb mit gemischten Versionen keine Schwierigkeiten auf. Dieses Kompatibilitätsversprechen soll für alle kommenden 1.x-Releases gelten. Erst bei einem Wechsel der Nummer vor dem Punkt ist mit einem Bruch zu rechnen.

Auf den Zeitplan für eine 2.0-Release angesprochen, reagierten die Projektverantwortlichen ausweichend. Es gibt wohl interne Diskussionen darüber, wie eine solche Version aussehen könnte, konkrete Pläne bestehen aber noch nicht. Die Einserlinie wird also wohl noch einige Jahre fortgeführt. Innerhalb dieser Linie soll es, wie beim Umstieg auf 1.5, Online-Migrationspfade geben. Nur wer das Backend wechseln (Datenbank oder Dateisystem), umorganisieren oder kompaktere Formate nutzen möchte, muss das Repository auf die Platte schreiben und wieder einspielen.

Fazit

Subversion wächst aus der Rolle des CVS-Nachfolgers heraus und schickt sich an, neue Nutzergruppen zu erschließen. Das aktuelle Release dürfte vor allem kommerzielle Anwender beeindrucken, aber auch im Open-Source-Umfeld werden die neuen Features sicherlich Anklang finden. Zudem ist die Integration in Entwicklungsumgebungen wie Eclipse oder Apples Xcode inzwischen praktisch komplett.

Mit dem Merge Tracking beschreitet Subversion neue Wege und versucht, die besten Features der verteilten Versionsverwaltung in sein zentralistisches Modell zu integrieren. Das aktuelle Release ist ein erster Schritt, in den Folgeversionen müssen die Entwickler belegen, ob sie ihre großen Ziele erreichen.

Die Zeit dürfte zeigen, inwieweit es gelingt, den Vorsprung vor den verteilten Versionsverwaltungssystemen zu halten. Der Abstand verringert sich nicht zuletzt dadurch, dass die Integration verteilter Versionsverwaltungssysteme in IDEs wie Eclipse besser wird und andere Bereiche wie Build Management sowie Continuous Integration folgen. Momentan hat hier Subversion aber noch deutlich die Nase vorn. (ka)

KAI GELLIEN

ist als Systemingenieur im Java- und C++-Umfeld tätig. Seine Schwerpunkte sind Projektinfrastruktur, agile Methoden und objektorientierte Softwareentwicklung.

ANDREAS LEIBL

ist freiberuflich als Systemberater für Unix-Systeme tätig, mit Schwerpunkt AIX und HACMP sowie Linux.

Literatur

[1] Andreas Leibl; CVS Reloaded; Versionsverwaltung mit Subversion 1.0, *iX* 08/04, S. 78

[2] Kai Gellien, Andreas Leibl; Subversion reloaded: SVN 1.3: Neue Features und grafische Frontends; *iX* 07/06, S. 78

Onlinequellen

Subversion	subversion.tigris.org
Mercurial(Hg)	www.selenic.com/mercurial/wiki/index.cgi/Mercurial
Merge Tracking	merge-tracking.open.collab.net

Berufliche Eignung des preiswerten Eee PC 4G von Asus

Leicht befunden

Martin Schmitz

Bei einem Notebook, das ohne Festplatte auskommt und weniger als 300 Euro kostet, drängt sich die Frage auf, ob es sich nur um ein Spielzeug handelt oder ob man es für berufliche Anwendungen gebrauchen kann und wenn, für welche.

Vor der Markteinführung des Eee PC 4G von Asus in Deutschland entwickelte sich im Internet bereits ein Hype um das kleine und preiswerte Gerät. Die drei „E“ im Namen stehen für „Easy to Learn, Work, and Play, Excellent Internet Experience, Excellent On-the-Go“. Was steckt dahinter, und ist der kleine Alleskönner vielleicht sogar für den professionellen Einsatz geeignet?

Zunächst zu den technischen Details: Easy stimmt auf jeden Fall, was Gewicht und Größe angeht: Der Eee PC wiegt etwas weniger als 1 kg und misst 225 × 165 × 35 mm, braucht somit kaum mehr Grundfläche als ein DIN-A5-Blatt. In das durchaus solide gearbeitete Gerät hat Asus als Prozessor einen 900 MHz schnellen Celeron 353 ULV und als Chipset den 910 GML eingebaut, beide von Intel. Zur Grundausstattung des Eee PC 4G gehören 512 MByte DDR2-RAM, eine 4 GByte große Flash-Disk und ein 7-Zoll-LCD als Bildschirm.

Das mutet auf den ersten Blick recht wenig an. Aber das vorinstallierte Betriebssystem, basierend auf der Linux-Distribution Xandros 4.0, fährt dank der Flash-Disk zügig und lautlos hoch. Der Widescreen mit einer Auflösung von 800 × 480 überrascht durch seine gut lesbare Darstellung. Zur weiteren Ausstattung gehören drei USB-2.0-Ports, WLAN, LAN- und Modem-Anschluss, Monitorausgang und SD-Steckplatz sowie eine integrierte 0,3-Megapixel-Kamera. Es fehlt somit nur ein optisches Laufwerk, was man aber angesichts des geringen Gewichts durchaus akzeptieren kann.

Asus hat weitere Varianten im Programm, die aber in Deutschland (noch) nicht erhältlich sind, etwa der Eee PC 2G mit halb oder der Eee PC 8G mit doppelt so großer Flash-Disk. Auf allen Modellen lässt sich Windows XP nachinstallieren, eine mehrseitige Anleitung ist dabei.

Umfangreiches Angebot an Software

Asus liefert den Eee PC 4G mit Open-Source-Software aus, die in einer ansprechenden Bedienoberfläche integriert ist. Laut Asus sind 40 Anwendungen vorinstalliert; eine kurze Suche über ein Smiley-Icon in den Eee-PC-Tipps oder im Internet führt schnell zu den nicht von der Oberfläche aus erreichbaren Programmen aus der KDE-Familie.

Die Anwendungen sind in sechs Tabs für Internet, Arbeit, Lernen, Spielen, Einstellungen und Favoriten eingeordnet. Mit der Bedienoberfläche kommen selbst Linux-Unkundige intuitiv zurecht. Einen Großteil des 4 GByte großen Flash-Speichers nimmt das Betriebssystem ein. Zur Installation zusätzlicher Softwarepakete bleibt dem Nutzer circa 1 GByte, das sich jedoch mit einer zusätzlichen SD-Speicherkarte leicht erweitern lässt.

Für berufliche Einsätze stellt der Eee PC unter Linux mit Open Office, Acrobat Reader, Firefox und Thunderbird alles Benötigte bereit. Sogar Skype ist vorbereitet und lässt sich mit den integrierten Komponenten Kamera, Mikrofon und Audio-Ausgang respektive Lautsprechern rechts und links des Bildschirms nutzen. Die Akkulaufzeit soll laut Asus bei 2,8 bis 3,5 Stunden liegen, dürfte aber unter WLAN-Dauerlast kürzer ausfallen.

Freundet man sich mit der kleinen und nicht ganz leichtgängigen Tastatur an, ist der Eee PC 4G für 299 Euro brutto eine Anschaffung wert, die sich durchaus für den Zugang zum Internet und für kleine Office-Arbeiten unterwegs eignet. Vor allem passt es mit seiner geringen Größe und dem niedrigen Gewicht immer noch ins Gepäck. Inzwischen hat der Eee PC sogar seine eigenen Sites, zum Beispiel: www.einfacheee.de. Asus' Eee PC 4G gefällt als kompaktes und preiswertes Subnotebook wegen seiner hohen Mobilität und seiner ausreichenden Grundausstattung: die kleine Alternative für den Job (eeepc.asus.com). (rh)

Lieferumfang und Preise

Eee PC 4G Sub-Notebook

Hardware: Celeron 353 ULV, 900 MHz; 512 MByte DDR2-SDRAM; 4 GByte Flash-Disk; Chipsatz: 910 GML (Intel); 800 × 480 VGA; WLAN; drei USB 2.0; 10/100-MBit-LAN-, Monitor-Anschluss; SD-Card-Slot; Kamera, 320 × 240 Pixel; Mikrofon, integrierte Lautsprecher

Software: Linux-Distribution Xandros, von Asus adaptiert; Open-Source-Software

Zubehör: Netzteil, Handbuch, Recovery-DVD, Neoprentasche, Akku (vier Zellen)

Hersteller: Asus (de.asus.com)

Preis: 299 Euro inkl. MwSt.

MARTIN SCHMITZ

ist Ingenieur im Bereich Anwendung und Entwicklung von präzisen Satelliten-Positionierungs- und Navigations-Systemen.

Embedded Datenbank Derby 10.4

Schlanker Speicher

Frank Pientka

Die Datenbank Derby ist so klein, dass sie auch in mobilen Geräten läuft. Version 10.4 des von der Apache-Foundation betreuten Produkts bringt unter anderem Kompatibilität mit JDBC 4.0 und XML-Verarbeitung.

Bei Apache Derby (db.apache.org/derby) handelt es sich um das ehemals kommerzielle Produkt Cloudscape der gleichnamigen Firma. IBM übernahm sie und schenkte die Software der Apache-Foundation, die sie inzwischen unter ihrer Lizenz freigab. Die Entwicklung von Cloudscape gehört eng zur Entstehung von Java und JDBC, da es seit 1996 vollständig in Java geschrieben ist. Große Aufmerksamkeit erlangte Derby, als Sun es als JavaDB mit dem JDK 6.0 auslieferte. IBM will den Support für das Einzelprodukt Cloudscape 10.1 ab September 2008 einstellen und unterstützt dann nur noch Derby.

Bereits mit der Vorgänger-Version 10.3.1.4 erhöhten sich die Anforderungen an die Laufzeitumgebung auf J2SE 1.4 beziehungsweise J2ME/CDC/Foundation-Profil 1.1. Wer trotzdem noch die älteren Versionen einsetzen möchte, die auch Sun nicht mehr wartet, kann 10.2.2 verwenden.

Wenig Platz, leicht integrierbar

Java vererbt Derby seine Vor- und Nachteile. So ist die Datenbank auf allen Plattformen mit passender JVM verfügbar und getestet. Die Performance und der Ressourcenverbrauch verbesserten sich zwar von Version zu Version, hängen jedoch von der Güte der JVM-Implementierung ab. Intern setzt Derby eine SQL-Abfrage in Java-Bytecode um. Ihn kann die JVM wiederum mit ihren Mitteln optimieren.

Stärken von Derby sind sein geringer Platzbedarf (2 MByte auf der Platte, den der in Java integrierte Pack200-Algorithmus auf 600 KByte reduziert) und die einfache Integrierbarkeit in andere Produkte. So gehört es zu vielen Apache-Produkten (Geronimo, ActiveMQ, James, Jetspeed-2, Roller) und IBM-Software (Eclipse, Websphere Application Server) – oft unbemerkt.

Verwaltung mit API und Kommandozeile

Zur Verwaltung der Datenbank stehen ein Programmier-API und ein Kommandozeilenwerkzeug zur Verfügung. So lassen sich Datenbankaufgaben bei der Entwicklung zum Beispiel mit Ant automatisieren. Wer jedoch eine grafische Oberfläche vermisst, dem helfen das Open-Source-Werkzeug SquirrelSQL und die Report-Funktion von Openoffice weiter. Entwickler können die Data-Tool-Plattform von Eclipse nutzen, in die Derby als Standard-Datenbank integriert ist. So lassen sich einfach Tabellen anlegen und Daten abfragen.

Für den Betrieb im Einzelplatz-Modus ist nur eine Jar-Datei (*derby.jar*) im Klassenpfad erforderlich. Zur Aktualisierung genügt der Austausch dieser Jar-Datei. Möchte man auch die Datenbankdaten in das Format der neueren Version konvertieren, was Voraussetzung etwa für die Verwendung des XML-Datentyps ist, gibt man das beim Verbindungsaufbau an:

```
connect 'jdbc:derby:toursdb;upgrade=true'
```

Die Umwandlung erfolgt dadurch automatisch und transparent, und anschließend lassen sich neuere Funktionen und Datentypen benutzen. Gerade was die Verwendung nicht relationaler Daten betrifft, bietet die neue Derby-Version mit dem XML-Datentyp und dem virtuellen Tabellen-Interface (VTI) gute Integrationsmöglichkeiten. VTI erlaubt das Anbinden und Bearbeiten externer Quellen wie Datenbanken und Dateien mit SQL. Derby selbst nutzt VTI etwa zum Speichern interner Datenstrukturen. Außerdem bietet die aktuelle Version JMX (Java Management Extension) zur Verwaltung von Java-Anwendungen an.

Die mitgelieferten Beispiele zeigen, wie Derby externe Daten, die in verschiedenen Dateiformaten oder in einer anderen Datenbank vorliegen, über die VTI-Schnittstelle als Tabelle verwendet. Dadurch stehen alle SQL-Mittel

zum Suchen und Bearbeiten zur Verfügung, ohne dass man sich mit dem Format der Daten beschäftigen muss. Außerdem können die Inhalte der VTI-Tabellen mit anderen Tabellen verknüpft werden. Das ist ein mächtiges Werkzeug zum relativ einfachen Einbinden unstrukturierter Daten in eine Datenbank, ohne sie dorthin zu importieren. Da die VTI-Tabellen keine Indizes unterstützen, bietet sich dieses Verfahren bei kleinen Datenmengen an, die sich häufig ändern. Die mitgelieferten Beispiele demonstrieren das für Property-, XML- und Log-Dateien sowie für die Anbindung einer externen MySQL-Datenbanktabelle. Voraussetzung ist in jedem Fall eine Java-Klasse, die Methoden für den Lese- und gegebenenfalls Schreibzugriff auf die Datenquelle bereitstellt. Das Einbinden dieser Methoden übernehmen Stored Procedures. Das folgende Beispiel aus der Derby-Distribution nutzt die Stored Procedure *propertyFileVTI*, die eine Tabelle zurückliefert. Es findet alle nicht ins Deutsche übersetzten Fehlermeldungen:

```
SELECT * FROM TABLE(
 propertyFileVTI('messages_en.properties' ) )
 m_english
 WHERE m_english.messageID NOT IN (
  SELECT m_german.messageID
  FROM TABLE(
   propertyFileVTI('messages_de.properties' ) )
  m_german
);
```

JDBC 4.0 enthält einen XML-Datentyp samt geeigneten Funktionen für die Verarbeitung von XML-Dokumenten. Voraussetzung für seine Verwendung ist ein JAXP-Parser wie Xalan 2.7.0 im *CLASSPATH* der JVM. Den neuen XML-Datentyp aus SQL20003 unterstützt zumindest die Datenbank selbst, jedoch nicht der JDBC-Treiber. Trotzdem lässt er sich mit Derby verwenden. Dazu muss der XML-Spaltenwert

iX-Wertung

⊕ geringer Platzbedarf

⊕ JDBC4-Implementierung

⊕ Datentyp und Funktionen für XML-Dokumente

⊖ kein *UPDATE* auf XML-Teildokumente

⊖ nur zwei CPUs im Parallelbetrieb möglich

Listing 1: Stylesheet DumpSQL.xsl

```
<?xml version="1.0"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
            version="1.0"
   xmlns:sql="org.apache.xalan.lib.sql.XConnection"
   extension-element-prefixes="sql">
  <xsl:output method="html" indent="yes"/>
  <xsl:param name="driver"
     select="'org.apache.derby.jdbc.EmbeddedDriver'"/>
  <xsl:param name="datasource" select="'jdbc:derby:toursdb'"/>
  <xsl:param name="query" select="'SELECT * FROM CITIES'"/>
  <xsl:template match="/">
      <xsl:variable name="db" select="sql:new($driver, $datasource)"/>
      <xsl:variable name="table" select='sql:query($db, $query)'/>
      <xsl:copy-of select="$table" />
      <xsl:value-of select="sql:close($db)"/>
  </xsl:template>
</xsl:stylesheet>
```

des Abfrageergebnisses mit *XMLSERIALIZE* in einen *CLOB* oder String umgewandelt werden. Diesen holt wie üblich *getString* aus dem JDBC-*ResultSet*.

Schnittstelle für virtuelle Tabellen

Nach dem Anlegen einer Tabelle mit

```
CREATE TABLE myXmlTable
  (I INTEGER, XCOL XML);
```

und dem Eintragen eines XML-Fragments per

```
INSERT INTO myXmlTable(i, xcol)
   VALUES (7, XMLPARSE( DOCUMENT
     CAST ('<article>
       <title>First Article</title>
       <author>John Smith</author>
       <body>A very short article.</body>
     </article>' AS CLOB)
PRESERVE WHITESPACE));
```

kann man mit geeigneten XPath-Ausdrücken darauf zugreifen:

```
SELECT i, XMLSERIALIZE (xcol as CLOB)
   FROM myXmlTable
   WHERE XMLEXISTS('//author[text() =
   "John Smith"]'
      PASSING BY REF xcol);
```

Analog zu *INSERT*- funktionieren *UPDATE*-Statements, die allerdings bislang nur das gesamte XML-Dokument austauschen können. Als weiterer XML-Operator steht *XQUERY* zur Verfügung. Damit lassen sich Teile von XML-Dokumenten wie Spalten einer Tabelle in SQL-Befehlen verwenden. Obwohl diese XML-Fähigkeiten noch nicht an die klassischer Datenbanken wie DB2 heranreichen, bietet Derby hier mehr als manche Open-Source-Konkurrenten.

Zur XML/XSL-Verarbeitung dienen Erweiterungen für den XML-Parser Xerces und XSL-/XPath-Parser. Aus Xerces lässt sich Derby direkt aufrufen, und die Ergebnisse der Datenbankabfragen stehen im Stylesheet zur Verfügung. So wandelt

```
java org.apache.xalan.xslt.Process \
 -XSL DumpSQL.xsl>>DumpSQL.xml
```

den Inhalt einer Tabelle mithilfe des Stylesheet *DumpSQL.xsl* (Listing 1) in XML. Das Resultat kann man mit einem weiteren Stylesheet zum Beispiel nach HTML konvertieren. Das zeigt, dass Derby neue Möglichkeiten der XML-Verarbeitung ohne zusätzliche Programmierung bietet.

Die Verwendung von Java für Stored Procedures ist sinnvoll, wenn es um komplexe Funktionen für datenintensive oder sicherheitsrelevante Abfragen geht. Sie laufen schneller als eine außerhalb der Datenbank liegende Variante, denn das Übersetzen in Java-Bytecode findet bereits beim Speichern der Prozedur statt.

Zum Schutz der Daten oder für den Betrieb auf Geräten ohne eigene oder mit nur schwachen Sicherheitsmechanismen kann die Derby-Datenbank verschlüsseln. Als Standardalgorithmus dient dazu DES (Data Encryption Standard). Mehr Sicherheit bietet jedoch DESede (triple DES) oder ein anderer JCE-Encryption-Provider. Dadurch ist die Datenbank vor einem Ausspähen besser geschützt.

Ein Vorteil von Derby ist der mögliche Einsatz auf mobilen Geräten, da es keine Verwaltung erfordert. Andererseits kann es ohne Änderungen auch als Client-Server-Datenbank laufen. Allerdings ist die Leistungsfähigkeit bislang dadurch begrenzt, dass es maximal zwei CPUs verwendet. Eine weitere Einschränkung besteht bei der Verteilung der Daten: Datenbankdaten und Transaktionsdateien lassen sich nur auf zwei separate Platten verteilen.

Über das von IBM entwickelte DRDA-Protokoll (Distributed Relational Database Architecture) oder alternativ einen ODBC-Treiber kann Derby mit Datenbanken anderer Hersteller Verbindung aufnehmen und mit weiteren Programmiersprachen verwendet werden. Die beste Unterstützung gibt es jedoch für Java und JDBC: Derby ist für JDBC 4.0 die Referenzimplementierung. Da es aufwärtskompatibel zu DB2 ist, lassen sich Anwendungen leicht portieren, falls man Funktionen dieser „großen“ Datenbank benötigt.

Version 10.4 bietet erstmals Rollen zur Zusammenfassung von Benutzerrechten, was die Kompatibilität mit anderen SQL-Datenbanken und die Sicherheit erhöht. Verbesserungen gab es ebenfalls bei der Performance, etwa durch die Verwendung eines Cache für Statement und Sitzungsdaten im Client.

Fazit

Was die Unterstützung von Standards betrifft, so ist Derby insbesondere bei JDBC vielen Open-Source- und sogar manchem kommerziellen Konkurrenten voraus. Die neue Version verbessert zudem die Sicherheit, die Verwaltung und die Integrierbarkeit. Entwicklern erleichtert sie durch den integrierten XML-Datentyp und Funktionen für seine Verarbeitung die Tätigkeit. (ck)

Literatur

[1] Frank Pientka; Java-Programmierung; JDBC 4.0: Einfacher und SQL:2003-kompatibel; Frischzellenkur; *iX* 12/2006, S. 138

[2] Alexander Schatten, Marco Zapletal; Java-RDBMS; Aber bitte mit Java; Freie Datenbanken: Derby und hsqldb; *iX* 5/2005, S. 70

[3] Oliver Schmelzle; Java-Programmierung; Java Management Extensions; Verwaltungsdienst; *iX* 6/2003; S. 116

Onlinequellen

Derby	http://db.apache.org/derby/
VTI-Dokumentation	http://db.apache.org/derby/javadoc/engine/org/apache/derby/vti/package-summary.html
SQL-Kompatibilität	http://wiki.apache.org/db-derby/SQLvsDerbyFeatures
Eclipse Datatools	www.eclipse.org/datatools/
DRDA	www.dbazine.com/db2/db2-mfarticles/mullins-drda

AVMs VoIP-Gateway 5188

Fritz goes Business

Torsten Krüger



Vor allem für den privaten und SOHO-Kommunikationsbedarf hat AVM seine Fritzbox-Serie konzipiert. Nun legt der Hersteller nach und bietet mit dem VoIP-Gateway 5188 ein Produkt an, das die Bedürfnisse kleiner und mittelgroßer Firmen berücksichtigt.

AVMs VoIP-Gateway 5188 ist gewissermaßen die logische Fortführung der etablierten Fritzbox-Serie für die Anwendung im Firmenumfeld. Im Gegensatz zu den Consumer-Modellen verzichtet die „Fritzbox heavy“ auf analoge Telefonanschlüsse, stellt dafür aber insgesamt nicht weniger als acht ISDN-Ports zur Verfügung. Vier sind fest für den NT-Modus konfiguriert, etwa für den Anschluss von ISDN-TK-Anlagen. Die Speisespannung für die NT-Schnittstellen erzeugt das Gerät intern. Die vier externen Anschlüsse im TE-Modus stellen Verbindungen zu den vorhandenen Amtsleitungen her.

Auf dem VoIP-Gateway läuft die bekannte AVM-Linux-Umgebung, wobei für die ISDN-Sektion wie bei den Fritzboxen proprietäre Treiber zum Einsatz kommen. Der Telnet-Zugang lässt sich genauso freischalten wie bei den Fritzboxen und bietet Bastlern – aber leider auch Angreifern – über die Kommandozeile vollen Zugriff auf das System.

Der VoIP-Teil des 5188 ist im Gegensatz zu den Implementierungen in den Consumer-Geräten durchwahlfähig. Das VoIP-Gateway 5188 lässt sich deshalb an Anlagenanschlüssen betreiben – Fritzboxen arbeiten nur an Mehrgeräteanschlüssen. Darüber hinaus haben die AVM-Entwickler einen Ethernet-Switch mit 4 Ports und ein ADSL-Modem integriert. Wireless LAN stellt das Gerät jedoch nicht bereit.

DSL-Router inklusive

Den integrierten ADSL-Router hat AVM fest auf NAT-Betrieb konfiguriert. Allerdings berücksichtigt das VoIP-Gateway die Lebenswirklichkeit in Netzwerken deutscher KMU insoweit, als die ADSL-Router-Sektion auch ungenutzt bleiben kann. Das AVM 5188 kann sich so ins IP-Netz integrieren und die dort vorhandenen Router nutzen.

Leider lässt sich der 4-Port-Switch nicht auftrennen. Zwar kann der Nutzer im Betrieb als DSL-Router einen „Exposed Host“ einstellen, eine echte „Demilitarisierte Zone“ (DMZ) lässt sich mit dem 5188 jedoch nicht aufbauen.

Zusätzlich zur DSL-Routerfunktion kann der 5188 als Endpunkt für bis zu vier VPN-Tunnel dienen. Als Gegenstellen eignen sich PCs mit installiertem AVM-VPN-Client, aber auch Fritzboxen sowie Software und Geräte diverser anderer Anbieter. Tipps zur Konfiguration sind auf www.avm.de zu finden.

Zugangsdaten für bis zu 40 VoIP-Provider kann der Nutzer über das GUI eingeben. Außerdem lässt sich dort mit Wählregeln und Auswahlziffern festlegen, welches Rufziel das Gerät auf welchem Weg – sei es VoIP oder ISDN – kontaktieren soll. Über die Funktion lässt sich manuell auch ein rudimentäres Least-Cost-Routing realisieren, etwa indem man Gespräche mit der Vorwahl *001* – also nach Nordamerika – grundsätzlich über VoIP-Provider X aufbaut, während Gespräche zu Mobilrufnummern über einen günstigen Call-by-Call-Anbieter im Festnetz laufen. Automatisieren, etwa über das regelmäßige Herunterladen frischer LCR-Tabellen aus dem Internet, lässt sich die Funktion jedoch nicht.

Zusätzlich kann der Nutzer bestimmten Quellrufnummern beziehungsweise den angeschlossenen Geräten eine Verbindung fest zuordnen. Das ist zum Beispiel sinnvoll, wenn man an einer nachgelagerten TK-Anlage ein Faxgerät angeschlossen hat, das nur über das Festnetz einwandfrei funktioniert. Wie die Fritzboxen versendet das 5188 Faxe über VoIP-Verbindungen als G.711-kodierte Audiosignale; „echtes“ Fax-over-IP nach dem T.38-Protokoll ist nicht implementiert.

Leider enthält die Firmware des 5188 keinen SIP-Client. Darin unterscheidet sich das AVM VoIP-Gateway deutlich von ähnlichen Geräten, etwa denen von Inalp/Patton oder Audiocodes, die man auch als Gateways für einen VoIP-Softswitch wie Asterisk oder Bluesocket (früher Pingtel) betreiben kann – etwa um die Zahl der nutzbaren Leitungen zu erhöhen. Eine solche Funktion würde den 5188 bei einem Straßenpreis von rund 350 Euro ausgesprochen interessant machen.

Fazit

In seinem gegenwärtigen Zustand scheint AVM das 5188 als reines Konvergenzprodukt zu positionieren, das in Verbindung mit einer existierenden, klassischen TK-Anlage dem Investitionsschutz beim Umstieg auf VoIP dienen soll. Für Anwender, die bereits einen Softswitch betreiben, ist das AVM 5188 wegen des fehlenden SIP-Clients jedoch keine Option. Es erweckt allerdings nicht den Eindruck, dass AVM die Funktion absichtlich unterschlagen hätte – bei den Fritzboxen, die bei der Entwicklung Pate standen, fehlt sie ebenfalls. (mr)

TORSTEN KRÜGER

ist Geschäftsführer bei der ncore GmbH in Duisburg.





Mingle:
Planungssoftware für agile Projekte

Durchgemischt

Christian Weiss, Guido Zockoll

Herkömmliche Projektmanagementsysteme geben sich häufig etwas behäbig und unflexibel. Mingle versucht sich als schlanke und agile Variante und bringt als Planungswerkzeug die altbewährte Karteikarte ins Spiel.

Es gibt zahlreiche Werkzeuge für die Planung und Kontrolle von Projekten. Trotzdem können Microsofts altgediente Produkte Project und Excel wohl immer noch die meisten Einsätze vorweisen. Die Vorgaben für ein flexibles Projektmanagement, neuerdings gern mit dem Universalbegriff „agil“ versehen, erfüllen diese Programme jedoch nicht, denn hier sind schlanke Konzepte gefragt und keine riesigen Gantt-Diagramme. Mit kurzen Zyklen, im Fachjargon Iterationen oder Sprints, wechselnden Prioritäten und Anforderungen kommen die konventionellen Vertreter der Zunft nicht zurecht. Bislang eignen sich für solche Zwecke nur wenige Tools wie XPlanner und XPWeb. Leider geben auch die sich ein wenig gehemmt: Sie arbeiten ausschließlich mit einer festgelegten Terminologie und kooperieren nur mit bestimmten Vorgehensmodellen wie XP oder Scrum (siehe Kasten „Onlinequellen“).

Mingle von Thoughtworks, im Sommer 2006 erschienen und derzeit auf dem Versionsstand 1.1, sucht neue Wege. Statt Aufgaben in langen Listen zu verwalten, dient hier die Karteikarte als zentrales Planungswerkzeug (siehe Abbildung 1). Die komfortable Webanwendung stellt allen Beteiligten über eine Ajax-Oberfläche sämtliche Projektinformationen gesammelt an einem Ort zur Verfügung. Allen Beteiligten wird etwas geboten: Der Projektleiter kann den Fortschritt des Vorhabens kontrollieren, der Entwickler darf sich den Sourcecode ansehen, Kunden und Anwender erfassen ihre Anforderungen und können sich über das Projekt informieren. Als besondere Stärke wirft das Tool seine Anpassungsfähigkeit an beliebige Vorgehensmodelle in die Waagschale.

In vielen agilen Projekten planen die Teams ihre Aufgaben mit konventionellen Karteikarten aus Papier (zum Beispiel Task Cards in XP oder Backlog Items in Scrum). Sie werden üblicherweise nach bestimmten Merkmalen an eine Planungswand gepinnt und nach Bedarf im Projektverlauf für verschiedene Zwecke umsortiert. Teams, die sich im selben Raum aufhalten, können nach dieser Methode hervorragend arbeiten. Das Berichtswesen nach außen gestaltet sich allerdings schwierig, für verteilt organisierte Projektgruppen eignet sich das traditionelle Verfahren daher nicht.

Die traditionelle Karteikarte lebt

Mingle löst sich von den tabellarischen Darstellungen herkömmlicher Projektmanagement-Werkzeuge. Das Karteikartensystem erschließt sich dem Benutzer innerhalb eines Tages. Wer beispielsweise Microsofts Project vernünftig bedienen will, braucht eine Woche Schulung. Jede Karte können die Teammitglieder inhaltlich beschreiben und mit beliebig vielen Attributen ausstatten. Über die Definition des numerischen Attributs *Iteration* würden sie das Werkzeug beispielsweise für iterative Vorgehensmodelle anpassen.

Eine Planungswand stellt in der Regel nur einen bestimmten Aspekt dar. Etwa, wer gerade woran arbeitet, den Projektfortschritt oder welche Features welches Team in welcher Iteration fertigstellen soll. Mingle hingegen verwendet frei konfigurierbare Register, die dem Planer die Möglichkeit geben, seine Karten nach bestimmten Merkmalen zu filtern und zu ordnen. Jedes Register zeigt mithin eine andere Sicht auf die Planung.

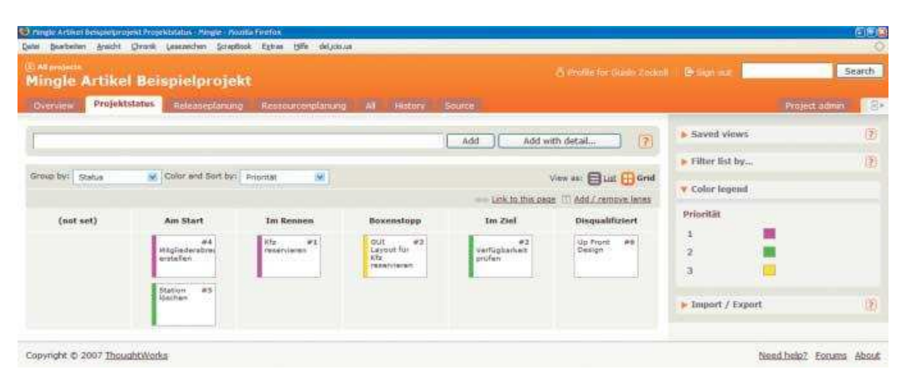
In den Registern kann das Werkzeug die Karten nach einem Attribut – zum Beispiel *Status* – in Spalten gruppieren und nach einem weiteren Attribut farblich hervorheben (etwa für unterschiedliche Prioritäten). Einfaches Verschieben der Karte mit der Maus in eine andere Spalte löst einen Statuswechsel aus. Steht die Ressourcenplanung im Vordergrund, könnte ein Register dies so darstellen: Spalte = Teammitglied, Farbe = geforderte Fähigkeit. Durch die Kombinationen von zwei Attributen entstehen einfach und schnell aussagekräftige Übersichten, die der Benutzer speichern und für den

Onlinequellen

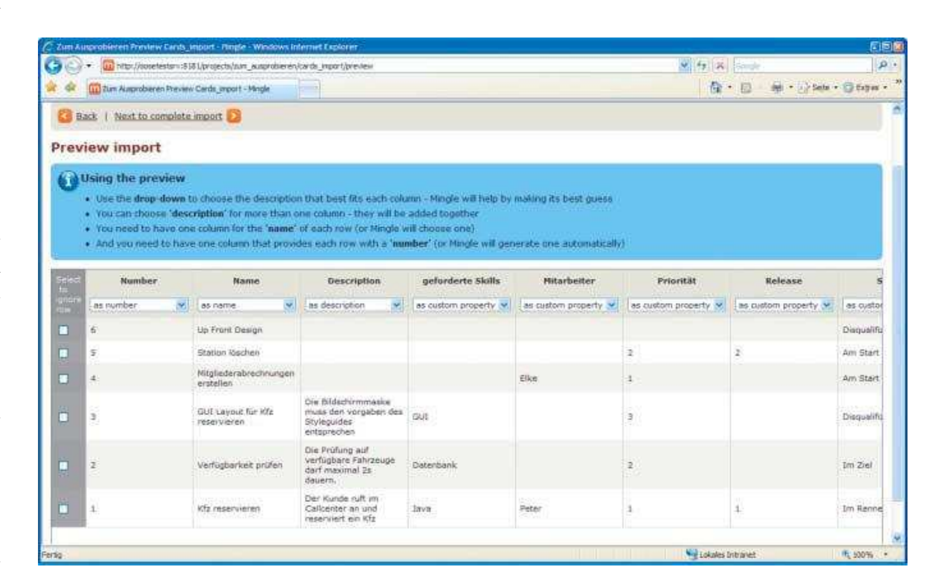
Mingle	studios.thoughtworks.com
XPlanner	www.xplanner.org
XPWeb	xpweb.sourceforge.net
XP-Prinzipien	c2.com/xp/DoTheSimplestThingThatCouldPossiblyWork.html

schnellen Zugriff als Tab-Reiter festlegen kann.

Die Übersichten geben einen guten Einblick in den Projektstatus. Manchmal muss es allerdings doch ein Tortendiagramm oder ein Chart sein. Zu diesem Zwecke bietet die Einstiegsseite frei definierbare Grafiken. Mit der eigenen Abfragesprache MQL (Mingle Query Language) lassen sich Attribute auswählen und die Ergebnisse aggregiert darstellen. Auf diese Weise ist der Benutzer in der Lage, sich eine Art Kommandostand zu bauen, der die wichtigsten Projektmetriken grafisch anzeigt.



Das übersichtliche und eingängige Karteikartensystem ist Mingles wichtigstes Projektplanungswerkzeug (Abb. 1).



Beim Import von Excel-Listen extrahiert das Werkzeug sinnvolle Attribute und wandelt die Zeilen in Karteikarten um (Abb. 2).

Systembefüllung via Excel

Der beste Weg, Karteikarten ins System zu bekommen, führt über eine Excel-Liste (siehe Abbildung 2). Mingle wandelt deren Zeilen in Karteikarten um. Umgekehrt geht es ebenso. Die Liste lässt sich per Cut & Paste in das Projektmanagementwerkzeug übertragen. Es versucht, in den Spalten sinnvolle Attribute wie *Id* oder *Name* zu erkennen und zu extrahieren. Alle unbekannten Spalten enden als sogenannte Custom Properties, die man ignorieren kann.

Als weiteres Features enthält Mingle ein Wiki sowie die Möglichkeit, eine Verbindung zum Versionskontrollsystem Subversion zu etablieren. IDs in den Subversion-Kommentaren zeigen auf die passenden Karten. Man kann ein Projekt als Schablone für weitere Projekte exportieren, die dann über die gleichen Attribute, Reports und Views verfügen. Drei Schablonen für verschiedene Projekttypen gehören zum Lieferumfang (Iterativ, XP und Scrum). Zudem Newsfeeds, E-Mail-Benachrichtigungen bei wichtigen Ereignissen, Projekthistorie und anderes mehr.

Eine Aufgabe in Mingle besteht aus mehreren Teilaufgaben. Diese einfache hierarchische Beziehung lässt sich in dem Tool nur schlecht abbilden. Zwar kann der Planer über selbst definierte Attribute Verweise auf übergeordnete Aufgaben erfassen, doch eine übersichtliche Darstellung, etwas in Form eines Baumes, gibt es nicht. Weiterhin fehlen eine deutsche Lokalisierung sowie die Option, auch andere Versionierungssysteme als Subversion anzubinden.

Ebenso ungewöhnlich wie das Werkzeug selbst erscheint Mingles Lizenzmodell. Open-Source-Projekte und nicht kommerzielle Organisationen dürfen das Tool kostenfrei benutzen. Kommerzielle Anwender bekommen die ersten fünf Lizenzen umsonst. Ab der sechsten möchte Thoughtworks 59 US-Dollar pro Monat und Benutzer haben – es geht also nur im Mietmodus.

Fazit

Das Projektmanagementwerkzeug Mingle eignet sich gut für die Planung und Kontrolle agiler Projekte. Zwar gibt es ähnliche Produkte (XPlanner und XPWeb), Mingle überzeugt jedoch durch Flexibilität, einfache Bedienung und kurze Einarbeitungszeit und folgt dem XP-Prinzip: „Tue das Einfachste, was die Anforderungen gerade eben erfüllt.“ Mit ihrem überzeugenden Karteikartensystem erfüllt die Software die meisten Anforderungen an eine professionelle Projektplanung auf elegante Weise. (jd)

CHRISTIAN WEISS

ist Geschäftsführer bei der oose GmbH in Hamburg

GUIDO ZOCKOLL

ist Geschäftsführer der EXPERTS@WORK GmbH in Hamburg.

iX-Wertung

⊕ Unabhängigkeit vom Vorgehensmodell

⊕ verständliches Karteikartensystem

⊕ Im- und Export von Excel-Listen

⊕ kostenlos für kleine sowie Open-Source-Projekte

⊖ keine übersichtliche Aufgabendarstellung

⊖ Lizenzen nur im Mietmodell

VoIP-Kommunikationsplattform für Unternehmen

Gruppenleiter

Patrick Harpes, Johannes Hermen



Teamfon bietet mit TeamSIP eine VoIP-Lösung, die nicht nur die klassische Telefonie ersetzen soll. Der Hersteller sieht sein Produkt als universelle, integrierte Kommunikationsanlage.

Dass Voice over IP weitaus mehr bieten kann als weniger Verkabelung und geringere Kosten, will die Firma Teamfon mit ihrem Produkt TeamSIP beweisen. Es soll über den bloßen Ersatz der klassischen Telefonzentrale hinausgehen. Seine auf Standards aufsetzende modulare Architektur bildet Geschäftsprozesse ab und bringt dabei unterschiedliche Kommunikationsformen unter einen Hut (siehe Abbildung 1). Teamfon bietet sein Produkt als Softwarepaket, als Appliance sowie gehostet an. Gegenstand der Untersuchung war die erstgenannte Variante.

In bestehende Applikationen lässt sich TeamSIP mit sogenannten Konnektoren integrieren, die es für den Client und den Server gibt. Client-Konnektoren enthalten Schnittstellen zu diversen Desktop-Anwendungen, etwa zu Outlook-Adressbüchern. Serverseitige stellen beispielsweise Schnittstellen zu ERP- und CRM-Systemen mit unterschiedlichen Protokollen bereit. Dabei führt TeamSIP weder neue Protokolle ein, noch erweitert es die existierenden. Telefondaten überträgt es per Session-Initiation-Protokoll (SIP), alle anderen Daten stellt es durch Webservices zur Verfügung.

Verbindungen zur Außenwelt

Im Zentrum von TeamSIP steht eine relationale Datenbank, die alle Daten und Konfigurationen speichert. Sowohl der Telefon- als auch der Integrations- und der IM-Server greifen darauf zu.

Der Telefonserver stellt alle Sprachdienste zur Verfügung. Eine wichtige Funktion ist die Verwaltung der Wahlpläne, mit denen der Nutzer das Routing der Telefongespräche beeinflussen kann. Zudem ist der Telefonserver zuständig für die Voice-Mailboxen der Teilnehmer. Sprachnachrichten können die Nutzer über das Web-Interface des Integrationsservers als WAV-Datei abrufen.

Ein weiteres Feature des Telefonservers sind die sogenannten „Queues“. Diese Warteschlangen besitzen eigene Telefonnummern und lassen sich dynamisch unterschiedlichen Personen zuweisen. Ist eine Queue definiert, kann ein Teilnehmer sich anmelden und die eingehenden Telefongespräche empfangen. Verlässt er das Büro, meldet er sich wieder ab. Ist niemand mehr angemeldet, kann das System dem Anrufer zum Beispiel einen Hinweis zu den Bürostunden geben. In Unternehmen mit vielen Filialen dürfte die Konferenzraum-Funktion beliebt sein. Man kann mit dem Telefonserver virtuelle Räume anlegen und jedem eine eigene Telefonnummer zuweisen. Dort können sich mehrere Teilnehmer „treffen“ und eine Konferenz abhalten.

Viele Dienste kombiniert

TeamSIPs Integrationsserver ist nicht nur für das Einbinden externer Applikationen zuständig. Er dient außerdem als Web-Frontend für das gesamte System. Die Webschnittstelle zur Verwaltung unterscheidet Administratoren und gewöhnliche Benutzer. Erstere können Wahlpläne erstellen, neue Nebenstellen anlegen oder zentrale, abteilungsweite sowie persönliche Telefonbücher anlegen und pflegen.

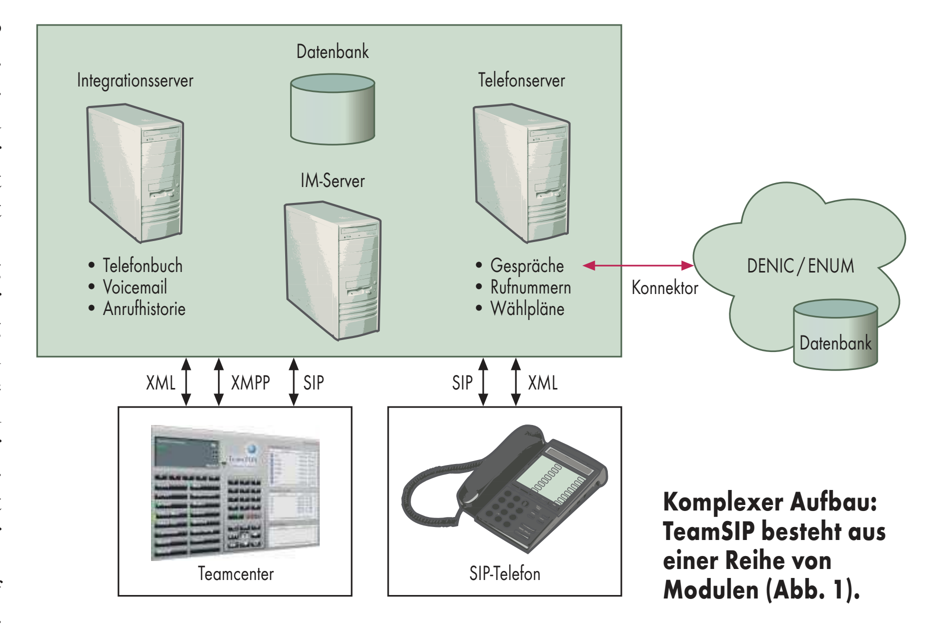
Alle Teilnehmer können per Browser ihre Sprachmailbox abhören, Kurzmitteilungen (SMS) verfassen und Informationen über die geführten und verpassten Telefongespräche einsehen. Außerdem lassen sich über die Webschnittstelle Umleitungen definieren und aktivieren. Bei allen Aktivitäten steht dem Nutzer ein integriertes Hilfesystem zur Seite.

Der Webserver unterstützt verschlüsselte Verbindungen via SSL beziehungsweise HTTPS. Allerdings hat der Hersteller die Funktion im Auslieferungszustand nicht aktiviert.

Neben VoIP beherrscht TeamSIP auch Instant Messaging (IM). Der integrierte IM-Server versteht das XMPP-Protokoll (Extensible Messaging and Presence Protocol) und erlaubt nicht nur den Austausch von Nachrichten mit anderen Teilnehmern, sondern stellt außerdem eine Präsenzanzeige bereit.

Least Cost Routing zur Ermittlung der günstigsten Verbindung ist seit der Liberalisierung des Tk-Marktes gang und gäbe. Um festzustellen, ob ein Teilnehmer auch per Internet-Telefonie erreichbar ist, kann TeamSIP bei einem ENUM-Server (tElephone NUmber Mapping) nachfragen (siehe Abbildung 2). Existiert dort kein Eintrag, lässt sich der Anruf nur über das Mobil- oder Festnetz routen.

Alle Serverkomponenten basieren auf Open-Source-Software, von der Datenbank MySQL bis zum Telefonserver Asterisk. Der Integrationsserver verwendet Apache/Tomcat, der IM-Server Jabber. Die Komponenten lassen sich auf einer Maschine installieren oder – bei höheren Skalierungsansprüchen – auf mehrere Rechner verteilen.



Komplexer Aufbau: TeamSIP besteht aus einer Reihe von Modulen (Abb. 1).

Softwaretelefon inklusive

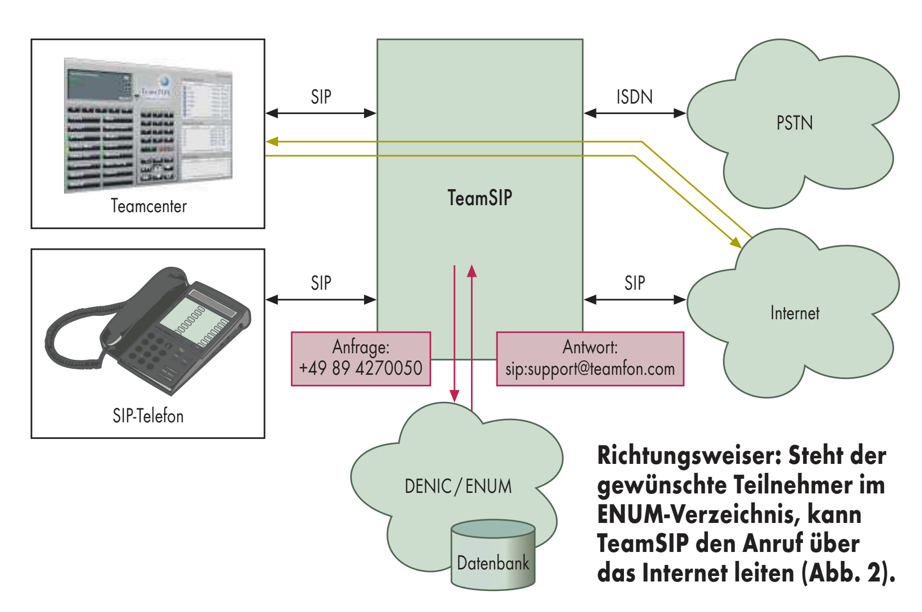
Da TeamSIP auf dem VoIP-Protokoll SIP basiert, sollte es mit jedem SIP-fähigen Telefon zusammenarbeiten. Unter dem Namen Teamcenter liefert der Hersteller außerdem ein erweitertes Softphone mit, das neben den Sprachdiensten Funktionen wie IM, SMS-Versand, hierarchische Telefonbücher, Kurzwahltasten, Statusanzeige et cetera besitzt (siehe Abbildung 3).

SIP-Telefon und Teamcenter lassen sich auch gemeinsam einsetzen. So kann der Nutzer etwa eine Nummer aus dem Teamcenter-Telefonbuch wählen, das Gespräch jedoch mit dem SIP-Telefon führen. Konnektoren erlauben sowohl das Anzeigen von Teamcenter-Funktionen in anderen Applikationen, etwa des IM-Status im Adressbuch von Microsoft Outlook, als auch das Fernsteuern des Clients, zum Beispiel den Aufbau von Gesprächen aus anderen Programmen heraus.

Telefonbücher und Kontaktlisten anderer Anwendungen lassen sich ebenfalls durch Konnektoren in Teamcenter integrieren. Da die Konnektoren-API des Clients für Kunden frei verfügbar ist, können sie Anpassungen an diverse Softwareprodukte selbst vornehmen.

Durch die client- und serverseitige Erweiterbarkeit lassen sich mit TeamSIP auch Callcenter-Applikationen realisieren, bei denen der Client bei einem Anruf Eingabemasken und Fragebögen einblendet, deren Ergebnisse sich über den Server in Datenbanken oder Applikationen zurückschreiben lassen. Ebenso wäre es möglich, bei eingehenden Anrufen Kundeninformationen aus anderen Systemen anzuzeigen. Die Übertragung der Daten zum Integrationsserver übernimmt Teamcenter, sodass man nur den serverseitigen Konnektor zur externen Anwendung neu zu schreiben braucht.

Mit der Installation des Servers sollte ein erfahrener Linux-/Unix-Systemadministrator keine Schwierigkeiten haben. Zunächst ist das Betriebssystem zu installieren – TeamSIP verlangt die kostenlose Linux-Distribution Fedora Core 6 als Unterbau. Anschließend muss der Admin mit *yum update* das System auf den aktuellen Stand bringen. Nach einem Reboot lässt sich das TeamSIP-Paket aus der Shell heraus installieren.



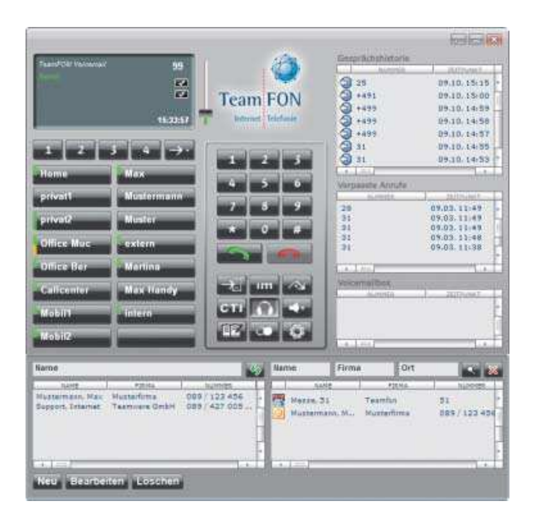
Richtungsweiser: Steht der gewünschte Teilnehmer im ENUM-Verzeichnis, kann TeamSIP den Anruf über das Internet leiten (Abb. 2).

Fachwissen ist hilfreich

Das Installationsskript fragt nach diversen Informationen wie dem Namen des Systems, der Landes- und der Ortsvorwahl. Bei Letzterer erwartet das Programm eine dreistellige Zahl, was etwa in Luxemburg zu Schwierigkeiten führt, da es dort keine Ortsvorwahl gibt. Künftige Versionen sollen toleranter sein.

Der Hersteller schickte gleich zwei Updates mit, die sich ohne Schwierigkeiten installieren ließen. Ein automatisches Update bietet Teamfon nicht an.

Anschließend muss der Administrator mit dem Browser das System einrichten. Mit ein paar Mausklicks kann er ein Abbild der Unternehmensstruktur



Armaturenbrett: Mit Teamcenter lassen sich alle Funktionen von TeamSIP nutzen (Abb. 3).

anlegen, Abteilungen definieren und interne Vorwahlen zuweisen. Danach lassen sich Teilnehmer eintragen und mit Nummern und Voice-Mailboxen versehen.

Weitaus schwieriger als das Einrichten des Basissystems gestaltet sich die erweiterte Konfiguration. Will der Administrator zum Beispiel virtuelle Räume anlegen, muss er manuell die Asterisk-Konfiguration ändern. Da VoIP-Lösungen für Unternehmen meist einer individuellen Anpassung bedürfen, bietet Teamfon einen – kostenpflichtigen – Installations- und Konfigurations-Service an.

Mit den zur Verfügung stehenden SIP-Telefonen, einem Grandstream GXP 2010 und einem Siemens Gigaset S450 IP DECT, überzeugte die Sprachqualität sowohl bei internen Gesprächen als auch bei Verbindungen ins Festnetz. Beim Teamcenter hing sie hingegen stark vom verwendeten Headset ab. Teamfon empfiehlt USB-Headsets mit aktiver Rauschunterdrückung. Wer drahtlose Headsets bevorzugt, sollte eher DECT- als Bluetooth-Geräte verwenden. Zudem spielt der gewählte Codec eine wichtige Rolle. Zur Verfügung stehen G.711 (A-law und μ-law), G.726, GSM und ILBC.

Fazit

Unterm Strich findet man mit TeamSIP ein solides Komplettpaket für VoIP-Anwendungen in kleinen bis mittleren Unternehmen. Das Produkt kann durchaus mit denen anderer großer VoIP-Anbieter mithalten, ohne jedoch in deren Preisklasse zu spielen. Durch die Integration in bestehende Telefonie-Infrastrukturen ermöglicht es eine sanfte Migration von der klassischen Telefonanlage zu Voice over IP.

Zurzeit steht mit Teamcenter nur ein Client für Windows ab Version 2000 bereit. Jedoch lassen sich die Grundfunktionen auch mit jedem anderen SIP-Softphone nutzen. Telefonbücher und Voice-Mailbox sind zudem über das Web-Interface erreichbar, wobei Teamcenter jedoch wegen der guten Integration und nützlicher Features einen besseren Eindruck hinterließ.

Generell stellt sich bei TeamSIP wie bei allen VoIP-Systemen die Frage nach der Ausfallsicherheit. Erschwerend kommt im konkreten Fall die komplexe Architektur hinzu, bei der der Ausfall einer Komponente das System zum Erliegen bringen kann. TeamSIP erlaubt es derzeit nicht, den Telefon- oder IM-Server redundant auszulegen, und hat somit einen Single Point of Failure (SPoF). Aber immerhin bietet der Hersteller seinen Kunden einen 24-Stunden-Support an. (mr)

PATRICK HARPES UND JOHANNES HERMEN

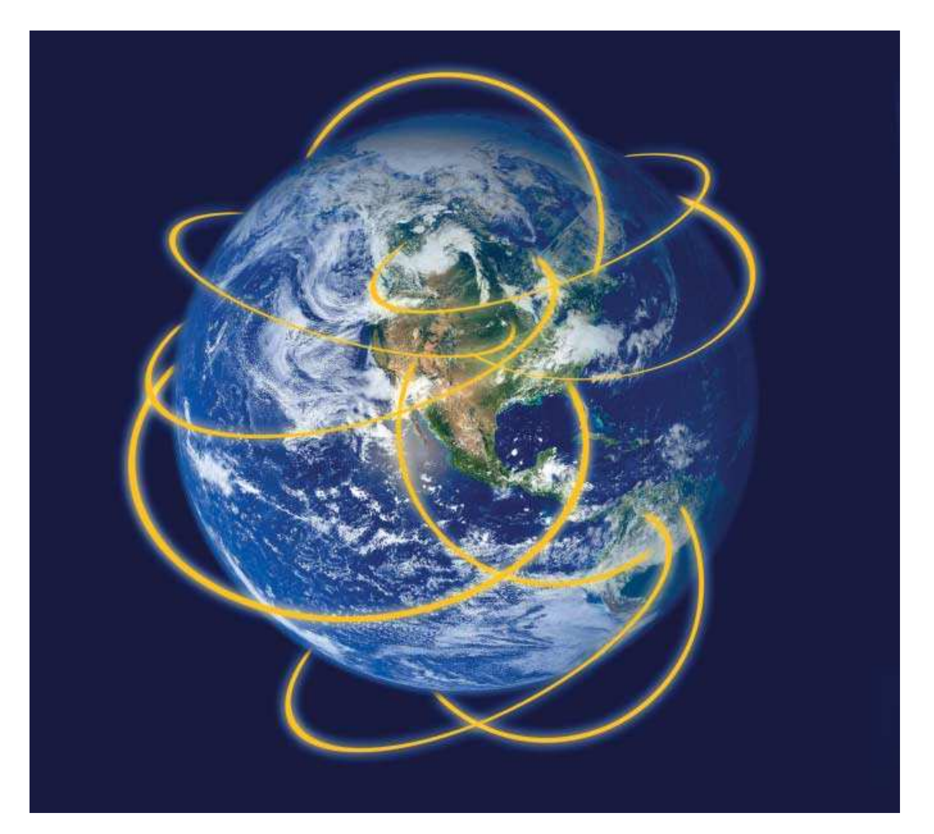
arbeiten im Luxemburger Forschungsinstitut Henri Tudor als Research Engineers.

iX-Wertung

⊕ großer Funktionsumfang
⊕ verwendet Standard-Protokolle
⊖ schwierige Konfiguration
⊖ mangelnde Ausfallsicherheit

Daten und Preise

Produkt: TeamSIP
Hersteller: Teamfon, www.Teamfon.com
Preise:
Softwarepaket: ab 800 Euro inkl. 5 Teilnehmerlizenzen
Appliance: ab 1200 Euro inkl. 5 Teilnehmerlizenzen
Teilnehmerlizenzen: 950/1700/3900 Euro (10/20/50 Teilnehmer)
Hosting: ab 59 Euro + circa 10 Euro pro Nebenstelle (monatlich)



Softwareprojekte managen mit EPF und xMDD

Agile Globalisierung

Eldar Sultanow

Unter dem Dach des Eclipse Process Framework finden viele verschiedene Projekttypen und Entwicklungsmethoden Platz. jABC von den Universitäten Dortmund und Potsdam erweitert EPF um grafische Modellierung und Kollaborationsfunktionen.

Das Eclipse Process Framework (EPF) stellt einen anpassbaren Rahmen für verschiedene agile Entwicklungsmethoden und Projekttypen zur Verfügung. Einige exemplarischer Prozesse gehören ebenso zum Leistungsumfang wie die notwendigen Werkzeuge für die praktische Arbeit. Die aktuelle Release 1.2 enthält den EPF Composer 1.2 sowie OpenUP/Basic 1.0 und bietet zahlreiche neue Funktionen. In Kombination mit dem ebenfalls agilen Kollaborationswerkzeug jABC (Java Application Building Center) eröffnet EPF interessante Optionen vor allem für kleine und mittlere Entwicklungsteams, die sowohl fest als auch selbstorganisierend sein können.

Komplett runderneuert präsentiert sich der Diagrammeditor. Er kann jetzt mit Swimlanes, Kontrollfluss-Labels, Freiformzeichnungen und Schriftstilen umgehen und Bilder im GIF-, JPEG- und BMP-Format speichern. Der ebenfalls überarbeitete Rich-Text-Editor erlaubt das Einfügen von Word-Dateien als Plain-Text sowie von Links und Bildern in der HTML-Ansicht. Seine HTML-Fehlermarkierungen und Korrekturfunktionen zeigen sich merklich verbessert. Der neue Prozesseditor ermöglicht das Ausblenden aller Tasks eines beliebigen Levels. Zudem unterstützt EPF jetzt Vista, den Internet Explorer 7 und Subversion. Publizierte Sites auf Applikationsservern können nun eine serverbasierte Suche umsetzen.

EPF hilft bei der Koordination von Projektabläufen, dem Versionsmanagement von Dokumentationen und stellt dafür standardisierte Vorgehensweisen zur Verfügung. Für kleine und mittelständische IT-Unternehmen, die sich international betätigen und Offshoring planen oder durchführen, ist EPF eine echte Alternative zu kostenpflichtigen Werkzeugen für das Softwareprojektmanagement.

Ideale Projekte zum Auslagern

Um für Offshoring infrage zu kommen, müssen Softwareprojekte vier wesentliche Kriterien erfüllen: Sie sollen über standardisierte Beschreibungsmittel verfügen, ein ausreichend großes Projektvolumen aufweisen, die Iterationshäufigkeit muss sich in Grenzen halten, und sie dürfen nicht übermäßig komplex sein. Ein zu umfangreiches Projekt kann sich, wenn Standardisierbarkeit fehlt, negativ auswirken, denn hier gewinnen Kommunikationsprobleme und Koordinationsaufwand schnell die Oberhand.

Vier Schlüsselfähigkeiten zeichnen EPF aus. Das Framework ist vielseitig einsetzbar, grundsätzliche Arbeitsschritte lassen sich in ähnlichen Projekten wiederverwenden, und eine standardisierte Beschreibungssprache dient als Grundlage für den Austausch auch über Firmengrenzen hinweg. Weiterhin besteht die Möglichkeit, Prozessmodelle mit geringem Aufwand unternehmensintern im gewünschten Corporate Design und in beliebten Formaten wie PDF oder HTML zu publizieren.

Onlinequellen

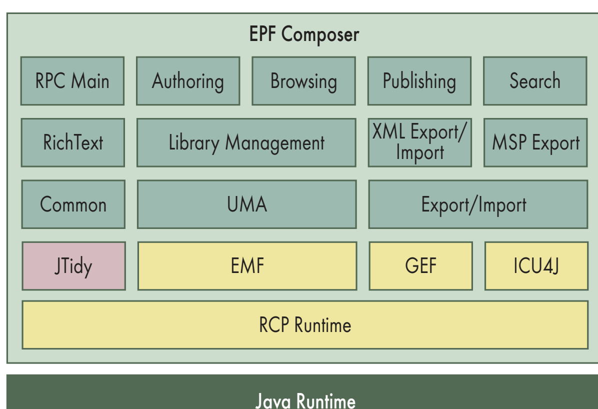
Eclipse Process Framework
www.eclipse.org/epf/

Kollaborationswerkzeug jABC
jabc.cs.uni-dortmund.de

EPF besteht aus dem EPF Composer (basiert auf Eclipse RCP, Rich Client Platform) sowie einer Sammlung von Prozessmodellen, nämlich OpenUP/Basic, dem agilen XP (Extreme Programming) und Scrum, einem iterativen Prozess, der die Prinzipen agiler Softwareerstellung in die Praxis überführt (Abbildung 1). Mit dem Composer arbeiten Prozessingenieure und Projektleiter, die für das Authoring, das Anpassen und das Veröffentlichen von Prozessen verantwortlich sind. Auch technisch wenig versiertes Personal soll dieses Werkzeug bedienen können.

iX-TRACT

- EPF, OpenUP/Basic und das Kollaborationswerkzeug jABC in Kombination helfen Entwicklungsteams bei der Projektorganisation auch von Offshore-Vorhaben.
- Für kleine und mittlere Teams bietet das Framework eine brauchbare Alternative zu kostenpflichtigen Konkurrenzprodukten.
- Zwar muss man sich anfangs intensiv in EPF einarbeiten, erhält als Belohnung aber sauber strukturierte Projekte.



In der vielschichtigen Architektur des EPF lässt sich der Aufbau von Eclipse wiedererkennen (Abb. 1).

Der Composer enthält ein Bündel von Software für die Definition, Pflege und Publikation von Prozessbeschreibungen und Verfahrensinhalten auf Basis der Unified Method Architecture (UMA), einer Weiterentwicklung des OMG-Standards SPEM (Software Process Engineering Metamodel). Das Werkzeug hat mehrere Zielgruppen: das Management, das den Überblick über Zeiträume und Kosten behalten will, den Entwickler, den die Beschreibungen über Prozesse und Metadaten interessieren, sowie den Projektverantwortlichen, der die Entwicklungsmethoden festlegt. Auch in der Lehre lässt sich das Framework gut einsetzen. Sein universeller Ansatz birgt natürlich einige Fallstricke. Der Einführungsaufwand ist groß, und OpenUP/Basic präsentiert sich vor allem dem Einsteiger aufgrund seines Umfangs als harter Brocken. Hinzu kommt, dass eine zentrale und frei zugängliche Dokumentation bisher fehlt.

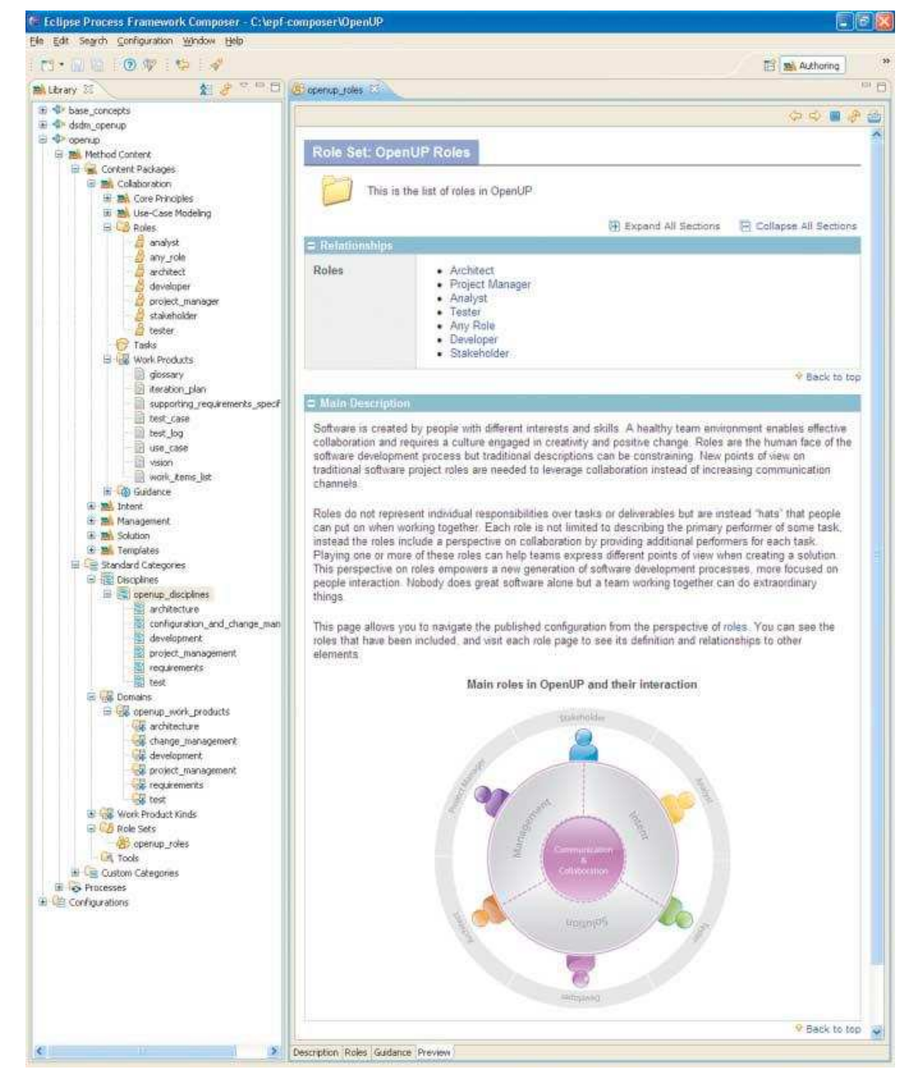
Jede gewünschte Entwicklungsmethode lässt sich via Plug-in in EPF verankern, vorhandene Plug-ins kann der Benutzer erweitern. Zu Letzteren gehören die schon erwähnten OpenUP/

Basic, XP und Scrum. Zum Herunterladen bereit liegen zudem die Agile Database Techniques (ADT) für die Entwicklung von Datenbankmodellen sowie das Agile Model Driven Development (AMDD). Beide erweitern den Basisprozess OpenUP/Basic (siehe „Onlinequellen“).

Das agile und leichtgewichtige OpenUP/Basic eignet sich gut für kleine Entwicklungsvorhaben und für Webprojekte. Obwohl der Prozess minimalistisch angelegt ist und sich ausschließlich um fundamentale Aspekte kümmert, ist er doch vollständig und erweiterbar. Das Vorgehensmodell bietet einen abgeschlossenen Prozesslebenszyklus und dient als Grundlage zum Anreichern der Entwicklungsabläufe mit zusätzlichen Funktionen und Programmen.

OpenUP/Basic deckt die Interessen aller Stakeholder (Anspruchsgruppen, Kunden) ab und verzichtet auf unproduktive Formalitäten. Der Prozess bietet eine zeitgemäße Herangehensweise für die Systementwicklung innerhalb eines bewährten und strukturierten Lebenszyklus. Er besitzt essenzielle Merkmale eines Unified Process, wie sich ihn die sogenannten drei Amigos und UML-Erfinder Grady Booch, James Rumbaugh und Ivar Jacobson ausgedacht haben. Sie schufen einen standardisierten, iterativ inkrementellen, architekturzentrierten Prozess, der Use Cases (Anwendungsfälle), Scenario-driven Development (anwendungsfallgetriebene Entwicklung) und Risikomanagement beinhaltet. Kurze Iterationen sollen ständiges Feedback erzeugen und so den Projektfortschritt sichtbar machen.

Der bekannte Rational Unified Process (RUP) liefert eine Referenzimplementierung eines Unified Process. Sein Lebenszyklus läuft über fünf Phasen: Einstieg (Geschäftsprozessmodellierung und Festlegung des Projektziels), Ausarbeitung (Projektplan, Grundzüge der Architektur), Konstruktion (Bauen des Produkts), Test und Auslieferung. Neben dem Projektmanagement unterstützt RUP das Konfigurations- und Änderungsmanagement (Change Management), eine Disziplin, die es ermöglicht, die IT-Infrastruktur kontrolliert, effizient und risikoarm anzupassen. OpenUP/Basic enthält die fünf Phasen in ähnlicher Form und ist die Referenzimplementierung für EPF.



Die Eclipse-typische GUI zeigt Rollen, Artefakte und Disziplinen von OpenUP/Basic (Abb. 2).

Klare Verhältnisse durch Rollenverteilung

OpenUP/Basic folgt einigen Kernprinzipien (siehe Tabelle „OpenUP/Basic-Kernelemente und ihre Zusammenhänge“), die als Grundlage für die Interpretation von Rollen, Produktentwicklung und Ausführen von Tasks dienen. Der Prozess teilt sich auf in zwei korrelierende Teile: den Methoden- und den Prozessinhalt. Im ersten legt man Rollen, Tasks, Artefakte und Anleitungen fest, unabhängig davon, wie diese später im Projektlebenszyklus zum Einsatz kommen. Im zweiten Bereich stellt der Entwickler die Methodeninhalte in einen zeitlichen Kontext. Der Prozess führt zudem Teilprozesse sowie eine Kollaborationsschicht ein.

Zusätzlich enthält OpenUP/Basic agile Konzepte wie Test-first Design (Test wird vor dem Code geschrieben), Continuous Integration (regelmäßiges, vollständiges Neubilden und Testen einer Anwendung), Time-boxed Iterations (jede Iteration hat eine strikte Deadline) und Refactoring (manuelle oder automatisierte Strukturanpassungen von Quelltexten). Letzteres soll die Lesbarkeit, Verständlichkeit, Wartbarkeit und Erweiterbarkeit des Codes verbessern. Wie RUP kennt OpenUP/Basic die Rollen Stakeholder, Analyst, Architekt, Entwickler, Projektmanager und Tester (Abbildung 3).

Die Methoden von OpenUP/Basic konzentrieren sich auf Anforderung, Analyse und Design, Implementierung, Test, Projektmanagement sowie Konfigurations- und Änderungsmanagement. Weiterführende Disziplinen wie Geschäftsprozessmodellierung oder ein ausgefeiltes Anforderungsmanagement fehlen hingegen, sind für kleinere Projekte allerdings auch nicht erforderlich.

Jedes Teammitglied erzeugt seiner Rolle entsprechend Artefakte, die jeweils Teilergebnisse beschreiben. Anhand dieser Dokumentation können alle Beteiligten das Projekt nachvollziehen,

OpenUP/Basic-Kernelemente und ihre Zusammenhänge

	Statement	Fokus auf	Umgang mit	OpenUP/Basic-Kernprinzipien	Methodeninhalte
Management (Projektleitung)	schnelle Reaktion bei Änderungswünschen, keine starre Planerfüllung	Geschäftssicht auf das Projekt	Monitoring, Führung, Risikominimierung	stetiges Feedback, kurze Iterationen	Projektmanagement
Ziel (Definition der Produktparameter)	Zusammenarbeit mit Kunden geht vor Vertragsverhandlungen	Anwendersicht auf das Projekt	Kommunikation, Aushandlung, Stakeholder-Belange	Ausbalancieren konkurrierender Prioritäten, Lösungsfindung	Anforderungs-, Konfigurations- und Änderungsmgmt., Test (Spezifikation der Test-Cases)
Lösung (Produkterstellung)	Softwareentwicklung hat Vorrang vor ausgedehnter Dokumentation	Sicht des Entwicklerteams	Erstellung und Verifikation technischer Produkte/Builds	Architekturfragen, technische Entscheidungen	Analyse & Design, Implementierung, Test (Programmieren der Testskripte)
Kollaboration (Fundament für Management, Ziel und Lösung)	Individuen und Interaktionen kommen vor Prozessen und Werkzeugen	Verantwortlichkeiten und Rollen der Teammitglieder	Zusammenarbeit im Team, klares Rollenverständnis, klare Verantwortlichkeiten	Entwicklung von Verfahren zur Teambildung, Förderung des Projektverständnisses	durchgehende Zusammenarbeit im Projekt, gemeinsame Artefakte

kontrollieren und Kollegen einarbeiten. Zudem bildet sie die Kommunikationplattform für die verschiedenen Rollen. Artefakte umfassen Quellcode, ausführbaren Binärcode und Dokumente mit formalen Systembeschreibungen (Diagramme und Metadatenkataloge). Die Kontrolle des Projekts mittels der Artefakte schließt eine dreistufige Qualitätsprüfung ein: statische Quellcodeanalyse, Modultests auf dem Binärcode sowie Durchsicht der Dokumente anhand von Checklisten.

Folgende Artefakte erstellt und modifiziert der Entwickler innerhalb von Teilprozessen: Use Cases, Glossar, Vorstellungen des Kunden (Vision), To-do-Liste, Test-Log und Testcase-Dokument (Abbildung 2 im Baum rechts unter *Work Products*). Weiter benutzt er informelle Darstellungen wie Screenshots, Whiteboards, Modellskizzen mit UML, Simulationen und ausführbare Prototypen. Sogenannte Capability Pattern kümmern sich um allgemeine Projektbelange. Die Muster können auf einzelne Bereiche, etwa Iterationsmanagement, Projektinitialisierung oder Architekturdefinitionen spezialisiert sein. Beispielsweise verwenden Projektmanager das Development Solution Pattern für Planungs- und Berichterstattungszwecke.

Gute Zusammenarbeit mit jABC

Neben Dokumentenmanagement und IT-Sicherheit nimmt das Collaboration Management eine Schlüsselstellung in internationalen Projekten ein. Hierfür eignet sich jABC, das von den Universitäten Dortmund und Potsdam entwickelt wird. Das Werkzeug existiert in einer freien (für Lehre und Forschung) sowie in einer kommerziellen Variante (Preise nach Absprache) und ist auf Anfrage von Prof. Tiziana Margaria erhältlich (siehe Kasten „Onlinequellen“). Eine im Web frei verfügbare Version ist geplant.

jABC basiert auf dem Modellierungsprozess xMDD (Extreme Model-driven Development, eine Weiterentwicklung des LPC, Lightweight Process Coordination). Für die grafische Modellierung verwendet jABC sogenannte SIBs (Service Independent Building Blocks) – serviceunabhängige Programmeinheiten, die sich sowohl in gleichen als auch unterschiedlichen Diensten wiederverwenden lassen, da sie nur deutlich abgegrenzte Funktionen bereitstellen. SIBs sind kompatibel zu allen Java-Sicherheitsstandards. Im jABC-Framework verbindet der Entwickler SIBs durch Kanten und kombiniert sie zu Flussgraph-ähnlichen Strukturen. Die Plug-ins verschiedener Hersteller, die OpenUP/Basic erweitern, bieten sowohl umfassende Techniken wie MDD als auch kleine, spezielle wie ADT.

xMDD erweitert andere Prozesse um eine Koordinationsschicht. Sie lässt sich durch Anordnung vordefinierter SIBs per Drag & Drop aufbauen. Der Modellierungsprozess setzt acht Aspekte um, die moderne Softwareentwicklungsmethoden wie OpenUP/Basic auszeichnen [1], [2]:

Einfachheit: Der Prozess konzentriert sich auf Anwender ohne Programmiererfahrung.

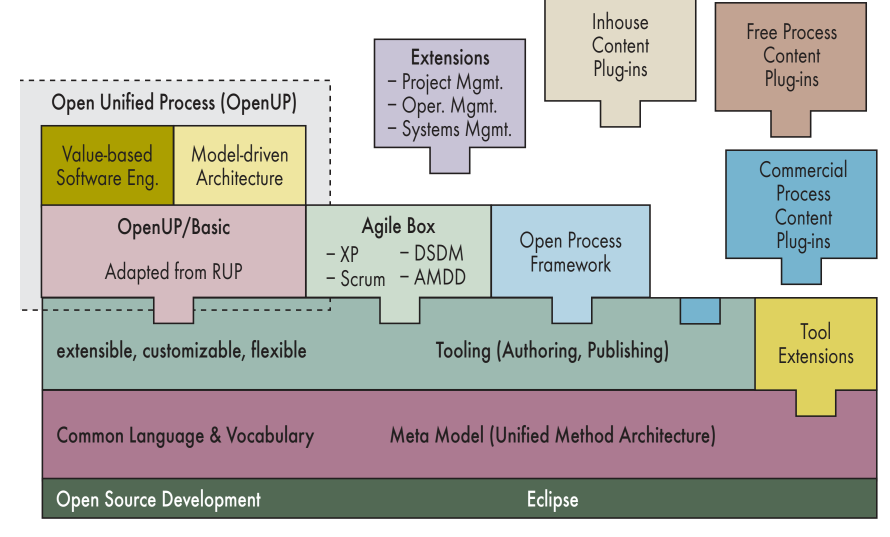
Flexibilität: Änderungen am Softwaremodell sind eingeplant (agile Softwareentwicklung).

Konsistenz: Dem kompletten jABC-Entwicklungsprozess liegt immer ein gemeinsames Softwaremodell zugrunde.

Anpassbarkeit: Die xMDD-Komponenten lassen sich umbenennen oder umstrukturieren, um den Namenskonventionen und Bedürfnissen der Fachanwender (beispielsweise Statistiker oder Biologen) zu entsprechen.

Verifikation: Techniken wie Local- und Modelchecking unterstützen den Benutzer. Idee ist, lokale und globale Bedingungen an ein Modell zu knüpfen.

Serviceorientierung: Bestehende Features oder Anwendungen lassen sich einfach in das Modell integrieren, indem



EPF-Ökosystem: OpenUP/Basic erweitert EPF um eine generische Schnittstelle für Prozess-Plug-ins (Abb. 3).

die Funktionen in einer xMDD-Komponente verpackt werden.

Ausführbarkeit: Ein Systemmodell kann auf verschiedenen Ebenen Code enthalten. Aus SIBs lässt sich an beliebiger Stelle ausführbarer Code generieren – über EJB3-konforme, annotationsbasierte O/R-Mappings bis hin zu Service-Rumpfklassen (Skeletons).

Universalität: Das Framework nutzt Java als Basis. Die Interoperabilität zu anderen Frameworks wie .Net ist aufgrund der Serviceorientierung gegeben.

xMDD bietet zwei wesentliche Rollen, die sich in EPF integrieren lassen und die Rollen von OpenUP/Basic ergänzen: Einen SIB-Fachmann sowie einen Experten, der die Programmanforderungen aus Anwendersicht formuliert. Letzterer konstruiert ein Modell aus bestehenden SIBs und definiert bei Bedarf neue (Name, Parameter und Kanten) mit jABCs SIBCreator-Plugin. Beide Rolleninhaber arbeiten selbstverständlich zusammen.

Eine SIB-Klasse ist unabhängig von ihren Anwendungsfunktionen zu implementieren (etwa mit Reflections für Zugriffe auf externe Funktionsbibliotheken). Dies ist erforderlich, damit für die Modellierung SIB-Klassen in die Laufzeitumgebung eines beliebigen Rechners geladen werden können – selbst wenn die Bibliotheken noch fehlen, die das Programm im späteren Produktivbetrieb benötigt. Die bei der Modellierung erstellten Graphenmodelle lassen sich wiederum als SIB verstehen und auf einer abstrakteren Modellierungsebene verwenden. Gleichermaßen lässt sich ein SIB zu einem Modell verfeinern, das eine detaillierte Sicht auf seine eigenen Anwendungsfunktionen bietet. Diese hierarchische Betrachtungsweise ermöglicht sowohl ein Top-down- als auch ein Bottom-up-Vorgehen im Modellierungsprozess.

Fazit

EPF, OpenUP/Basic und jABC bilden eine Werkzeugkombination, die dem agilen Ansatz folgt und über das übliche Softwareprojektmanagement hinaus internationale Entwicklungsvorhaben unterstützt. Der Modellierungsprozess xMDD verwendet SIBs als standardisiertes Beschreibungsmittel von Systembausteinen, die sich an verschiedenen Projektstandorten verwenden, auswerten und weiterverarbeiten lassen. Obwohl die EPF-Einführung mit einigen Aufwand verbunden ist, können vor allem kleine und mittlere Entwicklungsteams ihre Projekte damit gut strukturieren und koordinieren. (jd)

ELDAR SULTANOW

arbeitet als J2EE-Entwickler/Architekt bei der Producto AG in Berlin.

Literatur

[1] Tiziana Margaria; Service Is in the Eyes of the Beholder; University of Potsdam Guest Editor’s Introduction (on Service Orientation); IEEE Computer, November 2007 (Vol. 40, No. 11)

[2] Tiziana Margaria, Bernhard Steffen; Service Engineering: Linking Business and IT; IEEE Computer, October 2006 (Vol. 39, No. 10)

Suns T5220 mit T2-Prozessor

Der Niagara-Fall

Ralph Hülsenbusch

Hinter dem Codenamen Niagara 2 verbirgt sich ein Prozessor, der mehr auf dem Kerbholz hat, als nur mit Zahlen zu jonglieren. Das ruft unweigerlich die Ermittler auf den Plan, um zu prüfen, wo und wie man mit dem UltraSPARC T2 rechnen muss. Auf einer T5220 fand das Treffen statt, das Unvorhersehbares ans Licht brachte.



Seit Sun Microsystems unter dem Decknamen Niagara den UltraSPARC T1 mit besonderem Auftrag aussandte, kursieren Gerüchte über dessen Eignung fürs Geschäft. Er sei nur ein Lückenbüßer, hieß es, nachdem die Familie Fujitsu Siemens Computers mit dem SPARC64 VI Suns geplanten Coup UltraSPARC V aus dem Rennen warf und SPARC-VI-Nachfolger Rock auf sich warten lässt – von 2009 ist inzwischen die Rede. Wer die Akten über die Beziehungen der SPARCs untereinander einsehen möchte, kann das in den nicht geheimen Papieren der Sparc International tun (www.sparc.org). Das schafft schon das erste Gerücht aus der Welt: Sparc ist nicht (alleine) Sun, obwohl das Konzept der „Scalable Processor ARChitecture“ (SPARC) 1985 bei Sun Microsystems in Palo Alto entstand. Seit einigen Jahren verfolgt das Unternehmen die Strategie, mit offenen Karten neue Partner zu gewinnen und andere ins Geschäft einzuweihen – das erinnert an die Epoche der Sparc-Clones in den 80ern. Im August 2007 stellte es das Design des Open Sparc T2 unter GPL-Lizenz und übergab es der Open-Source-Community (www.opensparc.net).

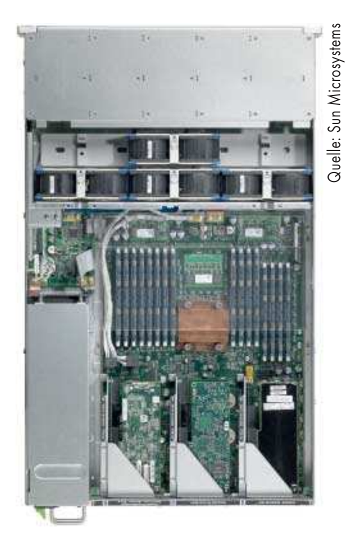
Mehr als ein Prozessor im Chip

Damit lüftet sich das Geheimnis um den Sonderfall Niagara. Im Herbst 2007 stellte Sun den Niagara 2 (T2) vor [1], ein System im Chip, konzipiert für gesicherte Webdienste und Virtualisierung. Die Ausrüstung beim Niagara 2 besteht aus acht Prozessorkernen mit einem gemeinsamen 4 MByte großen L2-Cache (3 MByte noch beim T1) nebst vier Memory-Management-Units für bis zu 64 FB-DIMMS, zwei 10-Gigabit-Ethernet-Ports, einer PCIe-Schnittstelle und einem Hypervisor für bis zu 64 virtuelle Domains. Während der T1 pro Core vier Threads verarbeiten konnte [2], schafft der T2 nun acht – in der Summe 64 Rechenaufgaben, die eine CPU zugleich bewältigt. Außerdem besitzt der T2 acht Floating Point Units, beim T1 war es nur eine. Das entzieht dem zweiten Gerücht den Nährboden: Der Niagara 2 ist durchaus für Gleitkommaberechnungen zu gebrauchen, Sun selbst ermittelte 62,3 SPECfp_rate2006. Der T2 führt dort die Rangliste der 1-Chip-CPUs im Gleitkommabereich an.

Aber der T2 hat noch weitere Trümpfe im Ärmel: Er besitzt jetzt zwei ALUs (Arithmetisch-Logische Einheiten) pro Core mit je einer achtstufigen Pipeline (statt bisher sechs) und acht Verschlüsselungseinheiten, pro Core eine. Sun hat damit einen besonderen Deal gelandet: mit 78,5 SPECint_rate2006 ist er weltweit derzeit der schnellste Chip, obwohl ihm Intels Xeon mit vier und IBMs Power6 mit zwei Cores im Nacken sitzen. Beim T2 steigt der Energiebedarf im Extremfall auf 123 W. Der T1 begnügte sich noch mit 72 W. Das Herz des T2 schlägt im 1,2- oder 1,4 GHz-Takt in den Coolthreads-Servern T5210 und T5220, der Blade T6320 sowie in den Telco-Pendants Netra Blade CP3260 und Rackserver T5220.

Zu leicht befunden

Eine verlockende Gelegenheit, T2 zu stellen, bot sich an der Universität Ulm, unterstützt von Sun Microsystems Deutschland. Ein T5220 mit 32 GByte RAM und 1,2 GHz schnellem UltraSPARC T2 stand per SSH zur Verfügung, betreut von Thomas Nau,



Kuschelig: In dem 2-U-Gehäuse drängen sich zweimal acht Bänke mit FB-DIMMs an die Niagara 2 (Abb. 1).



Etagere: Mehrere PCI-Slots übereinander geben Raum für bis zu sechs Karten, mit denen sich die Anbindung an SAN und Netz ausbauen lassen (Abb. 2).

iX-Autor und Leiter der Abteilung Infrastruktur des Kommunikations- und Informationszentrums, ein Zusammenschluss des Rechenzentrums mit anderen Abteilungen wie der Bibliothek, der Telekommunikation und weiteren an der Universität Ulm. Er hatte die Vorbereitung des Systems übernommen, die Compiler installiert und das Betriebssystem den Vorgaben entsprechend eingerichtet. In der ersten Sitzung ging es darum, den SPEC-Resultaten auf den Zahn zu fühlen. Zum Jahreswechsel war auf der Website der SPEC noch keine Veröffentlichung zu finden. Die Konfiguration der Compiler-Optionen für Suns (Forte) Compiler orientierte sich somit vorerst an früheren Vorgaben.

Und 32 waren nicht genug

Erste Verdachtsmomente kamen auf, als der Job für SPECint_base2006 erst nach drei Tagen erledigt war und SPECfp_base2006 den ersten Test selbst nach zwei Tagen noch nicht abgeschlossen hatte. Erst ein Herabsetzen der Optimierung führte zu Ergebnissen. Zwar mag eine Einzelbefragung mit nur einem Thread dem Können von T2 nicht entsprechen, aber die Antwort „2,14 SPECint_base2006“ verblüfft. Die Rechenleistung liegt unter der einer UltraSparc III in einer Sun Fire 3800 (August 2006) und etwa beim Doppelten der CPU2006-Referenz, einer UltraSparc II. Ein schrittweises Heraufsetzen der Optimierung und Öffnen von Schranken per *ulimit* konnten dem Aspiranten kein merklich besseres Ergebnis entlocken.

Hochrechnungen führen in die falsche Richtung, denn acht Threads auf einem Core führen nicht zu der achtfachen Rechenleistung, da sie der Core in einem Round-Robin-Verfahren bearbeitet. Kurz über den Daumen gepeilt erkennt man, dass 64 mal 2,14 in etwa das 1,75-Fache des von Sun ermittelten Wertes ergäbe.

Der eigentliche Haken verbirgt sich an anderer Stelle: Alle Messungen, die Sun und FSC zum T2 veröffentlicht haben, beziehen sich auf ein System mit 64 GByte Hauptspeicher und einer 1,4 GHz schnellen CPU, was einem Preissprung von 31 995 auf 58 995 US-$ gegenüber der Testplattform mit 1,2-GHz-CPU und 32 GByte RAM gleichkommt. Bemerkenswertes am Rande: FSC konnte mit dem GCC for Sun Solaris (*gcfss*) 83,9 SPECint_cpu2006 (peak) aus dem T2 herausholen. Dabei handelt es sich um ein reines GCC-Frontend für die Sun-Studio-Compiler (www.opensparc.org).

Fazit

Ohne Zweifel hat Sun mit dem Niagara 2 eine neue Technik auf den Markt gebracht: einen Prozessorchip, der nicht nur über acht Cores mit je acht HW-Threads verfügt, sondern in dem Ethernet- sowie PCI-Controller und vor allem pro Core eine Encryption Unit integriert sind. Vom „System in a Chip“ können vor allem Anwendungen profitieren, die eine Verschlüsselung brauchen und auf parallele Prozesse ausgelegt sind. Insofern eignet sich SPECs CPU2006 nur bedingt als Benchmark, da die Suite zwar parallele Jobs generiert, aber keine Threads verwendet.

Als das Dilemma im Test erwies sich die Schwierigkeit, mit solch große Anwendungen wie mit der CPU2006-Suite zu arbeiten. Bei voller Optimierung muss das Betriebssystem vorher so parametrisiert sein, dass der Compiler mit dem Hauptspeicher zurechtkommt. Wer versucht, die Suite mit allen 64 Threads laufen zu lassen, muss sich darüber im Klaren sein, dass er mindestens 1 GByte pro Prozess braucht – mit weniger als 64 GByte geht es nicht. Sun wirbt mit Benchmark-Ergebnissen, die von Niagara-Maschinen stammen, die mit 16-mal 4 GByte Hauptspeicher ausgerüstet waren. Das dürfte dem Einsatz in professionellen Umgebungen mit den dort üblichen Anwendungen kaum entsprechen. In anderen Disziplinen wie dem Java Business Benchmark (JBB2005) konnte die T2 sich bisher nur im Mittelfeld behaupten. (rh)

Literatur

[1] Susanne Nolte; Hardware; Kernobst; Multi-Core-Rechenwerke von AMD, Intel und Sun Microsystems; *iX* 9/2007, S. 14

[2] Thomas Nau; Multicore-Server; Sun Tzu; Suns 32-Wege-Server T2000 mit Ultra Sparc T1; *iX* 5/2006, S. 88

iX-Wertung

⊕ schnellster 8-Core-Prozessor

⊕ hohe Integration

⊖ hoher Speicherbedarf

Lieferumfang und Preise

Sparc Enterprise T5220 Server

Hardware: UltraSoarc T2, 8 Cores, 8 Threads pro Core, 1,2 GHz, 4 MByte L2-Cache; 32 GByte (16 × 2 GByte FB-DIMMs); zwei 146 GByte SAS-HDs; DVD-RW; vier 1-GByte-Ethernet, sechs PCIe (zwei x8, zwei x4, zwei x4 Lane oder XAUI); 2-U-Rack

Software: Solaris 10, Support für Linux (Ubuntu), Sun Forte Compiler, GCC for Sun Solaris (*gccfss*)

Hersteller/Anbieter: Sun Microsystems, www.sun.de

Preis: 25 500 Euro (Teststellung)



Desktops aus der Ferne nutzen

Fernbedienung

Ralph Hülsenbusch

Von Hardware über Software bis hin zu Dienstleistungen erstrecken sich die Angebote, mit denen man Computer aus der Ferne steuern und nutzen kann. Es gibt zwar eine Reihe kostenloser Softwarepakete, doch für die Nutzung von jedem x-beliebigen Zugang im Internet aus kommt man um kommerzielle Lösungen nicht herum.

Nicht nur Administratoren, sondern auch Nutzer einzelner Rechner oder ganzer Systemlandschaften können davon profitieren, wenn sie überall dort, wo ein Internetzugang bereitsteht, auf ihre Arbeitsumgebung zugreifen können. Die Spanne reicht vom einfachen Synchronisieren über gesicherte Zugänge zum System bis hin zum Büro im Netz, in dem Anbieter passende Software-Stacks zur Verfügung stellen. Application Service Provider (ASP) erleben eine Renaissance unter dem neuen Etikett „Software as a Service“ (SaaS), wohinter oft eine „Service Oriented Architecture“ (SOA) steht. Die ersten Versuche Ende der 90er etwa von Corel Office und Applix Anywhere [1] zeitigten wenig Erfolge mangels genügender Netzperformance. Neue Kompressionsverfahren und Netztechniken bieten heutzutage eine Grundlage, auf der Anwender Applikationen im Web ohne allzu große Verzögerungen im Antwortverhalten nutzen können.

Angesichts der Spannbreite des Themas bleibt eine Eingrenzung unumgänglich. Es geht hier um Software, mit der man seinen Desktop als Arbeitsmittel über das Internet nutzen kann. Hierfür gibt es drei Klassen:

Desktop zu Desktop

Die Arbeitsoberfläche des entfernten Rechners erscheint 1:1 auf dem Client (Duplicated Desktop), wobei entweder beide Anzeigen synchron laufen oder sich die auf dem remote Computer (Host) abschalten lässt. Dieses Verfahren erfordert Software auf beiden Seiten in der Art eines Client-Server-Modells. Dazu muss der Anwender die passenden Rechte auf beiden Systemen besitzen. Der Rechner im fernen Büro übernimmt die Rolle des Servers, der vor Ort die des Client.

Solche Methoden sind fester Bestandteil von Betriebssystemen wie Windows und Mac OS X. Bei den meisten Linux-Distributionen gehört die entsprechende Software mit zum Lieferumfang. Das Verfahren ist einfach in der Anwendung, aber unter Sicherheitsaspekten ausgesprochen heikel. Außerdem entsteht vor allem bei häufigem Orts- und Systemwechsel ein nicht zu unterschätzender Verwaltungsaufwand. Deshalb bieten eine Reihe von Firmen Alternativen an, die ein höheres Maß an Sicherheit versprechen und die Administration mithilfe

von Logs, Datenbanken und Reporting vereinfachen.
– Desktop-Umleitung (Remote Desktop): Systeme, die keinen eigenen Monitor-Anschluss besitzen (headless), was bei vielen neuartigen Servern und Embedded-Systemen, etwa bei Service-Prozessoren, der Fall ist, stellen ihre grafische Benutzer-Oberfläche samt Ein-/Ausgabe-Steuerung über das Netz dar. Meist geschieht das heutzutage über einen integrierten Webbrowser und Java, was das Installieren von Software auf der „Konsole“ erspart – sofern die Java-Version passt. Dazu muss aber die IP-Adresse des fernzusteuernden Rechners bekannt sein.
– Desktop-Emulation (Virtual Desktop): Da niemand weiß, über was für ein Gerät (Client) der Anwender für den Zugriff aus der Ferne gerade verfügt, packt eine Softwareschicht auf dem eigentlichen Arbeitsrechner (Host) den Desktop in einen überall nutzbaren Code, setzt somit eine virtuelle Maschine voraus, meist mit Java. Insofern stammt die Methode von den Headless-Systemen ab. Das verlangt von den Clients aber einiges an Leistung, vor allem bei der Grafik. Und da man Tastatur und Maus quasi doppelt nutzen muss – auf der lokalen und der entfernten Oberfläche – hapert es oft bei der Synchronisation.

Deswegen bieten eine Reihe von Firmen zusätzliche „native“ Software an, die man aber zunächst vor Ort auf dem jeweiligen System installieren muss. Das schränkt die Freiheit der Wahl auf die Geräte ein, auf denen man dazu die Rechte hat. Eine Alternative bieten Lösungen, bei denen ein Hoster die Weiterleitung des Desktops über das Internet übernimmt und ihn für jeden Browser bereitstellt.

Arbeitsplatz im Netz

– Desktop als Dienstleistung (Desktop-Provider): Völlig losgelöst vom Schreibtisch im Büro sind die Angebote von Dienstleistern (Providern), die dem Kunden eine mehr oder weniger komplette Arbeitsumgebung im Internet anbieten. Dazu muss sich der Anwender von der Bindung an den physischen Arbeitsplatz („mein Büro“) befreien können und sozusagen ganz ins Virtuelle umziehen. Der Vorteil liegt auf der Hand: keine Investitionen in eigene Hardware, deren Wartung und Sicherheitstechniken wie Firewalls, zusätzliche Server und Backups. Dem stehen berechtigte Zweifel an der Vertraulichkeit der eigenen Daten gegenüber. Zwar sind die Verschlüsselungs- und Authentifizierungsmethoden inzwischen ausgereift, aber das Rennen geht weiter: Jede weitere Sicherheitsstufe provoziert neue Angriffsmethoden, was wiederum zu mehr oder weniger öffentlichen Restriktionen und Kontrollen von staatlicher Seite führt.
– Desktop? Nein danke! (Virtual Application): Für die tägliche Arbeit sind die Desktops zu überfrachtet. Dabei geht es in allen Fällen nur um eins: Eine Maschine zu haben, die funktioniert, sprich die gewünschten Dinge erledigt. Dienstleistungen sind gefragt und da reicht es oft vollkommen, wenn bei der Sitzung im Netz nur die Geister erscheinen, die man ruft. Der Zugriff auf Anwendungen spielt die Hauptrolle. In diesem Bereich haben Firmen im Internet wie Google, Yahoo, Amazon, Ebay et cetera erste Ansätze zu bieten.

Durchs Netz geschleust

Auf dem ersten Stück des Weges gibt es ein breites Angebot für KVM oder IP – Keyboard-, Video- und Maussteuerung über das Internet-Protokoll. Solche Geräte, einst der Not fehlender serieller Konsolen bei Windows-Servern entwachsen, haben sich inzwischen zu Appliances gemausert, die mit eigenem Webserver an Bord die Fernbedienung ins Web verlagern, teils mit Java-, teils aus Performancegründen mit nativen Clients etwa von Adder, Avocent oder Raritan. *iX* berichtete 2005 darüber [3]. Die Remote Control Software gehört zur Hardware und ist nicht separat erhältlich. Bei näherem Hinsehen fällt aber in den meisten Fällen auf, dass die Hersteller sich aus dem Topf der Open Software bedienen.

iX-TRACT

- Remote-Control-Software erlaubt den Zugriff auf Rechner über das Netz von beliebiger Stelle aus.
- Das Spektrum reicht von der reinen Administration bis hin zur Nutzung von Anwendungen.
- Für den reinen Anwender sind Angebote, die den Desktop oder Applikationen im Internet bereitstellen, einfach zu nutzen.

Gestandene *iX*-Leser mit Unix-, Linux- oder BSD-Vorlieben dürften sich über die Frage wundern, was man für den Remote-Zugriff denn an kommerzieller Software braucht. Schließlich bieten SSH, Virtual Private Network (VPN) und Virtual Network Computing (VNC) nebst *rdesktop* alles, was man braucht. Mit etwas Hintergrundkenntnissen und Spaß am Probieren kann man sogar in gemischten Umgebungen mit Unix, Linux, BSD, Windows und Mac OS arbeiten, allerdings mit Zugeständnissen meist an die Tastatur-Emulationen aus der Ferne [4]. Windows-Nutzer können da nur mit den Schultern zucken. Alles, was sie für den Zugriff brauchen, ist im Gepäck: Remote Desktop, Terminalservices und *telnet*. Außerdem hat man schnell per Download ein Putty nebst WinSCP für den Zugriff auf und den Datenaustausch mit Nicht-Windows-Systemen installiert. Nur einen Haken hat die Sache, denn das funktioniert nur in definierten Umgebungen innerhalb von LANs, über VPN-Verbindungen mit festen IP-Adressen.

Gewachsenes Risiko

Inzwischen geht das alles weltweit übers Internet und gibt durchaus Anlass zur Sorge. Firewalls, IP-Filter und Verschlüsselungstechniken versuchen Schlimmstes zu verhindern. Doch selbst das klassische Out-of-Band-Netz, über das Administratoren innerhalb der eigenen IT-Struktur ihre Systeme unter Kontrolle halten, streckt seine Fühler ins weltweite Netz aus. Denn Zeit ist Geld, und wenn der Admin es mal eben vom nächsten Rechner aus richten kann, spart das eine Menge Geld und Nerven. Server besitzen heutzutage einen eigenen Service-Prozessor, teils on-board, teils in einer speziellen kleinen Huckepack-Platine mit eigenem Ethernet- und manchmal zusätzlichem seriellen Anschluss. Da setzen Hersteller wie Dell, FSC, HP, IBM und Sun ihre eigene Marke und verteilen die per IPMI gewonnenen Daten über Temperaturen, Spannungen und Lüfterdrehzahl auf proprietären Browser-Oberflächen. Über die kann, wer Zugang hat, Rechner aus der Ferne aus- und wieder einschalten.

An die Grenzen der Bedienbarkeit stößt man, wenn man etwa eine Konsole starten muss, um Software-Updates zu fahren oder Einstellungen am BIOS zu verändern. Bei den heutzutage

Remote Control Software

Produkt	Anyplace 4.3.1	GoTo My PC	HOB RD VPN	Laplink Everywhere
Hersteller	Anyplace Control	Citrix-Online	HOB GmbH	Laplink
Ort	Ukraine	Santa Barbara Cal./USA	Cadolzburg	Bellevue, Was./USA
Website	www.anyplace-control.com	www.gotomypc.com	www.hob.de	www.laplink.com
E-Mail	sales@anyplace-control.com	gotopro@citrixonline.com	marketing@hob.de	über Site
Kategorie	Remote Control (C/S)	Remote Desktop	Desktop Sharing	Remote Desktop
Sprache	mehrsprachig	englisch	mehrsprachig	mehrsprachig
Trial-Version	30 Tage, volle Version	30 Tage, 1 PC, (Abovertrag)	max. 4 Wochen	15 Tage, volle Version
freie Grundversion	nein	nein	nein	nein
Lizenz	pro Nutzer	pro PC	k. A.	pro PC
Upgrade u. Support	kostenpflichtig	k. A.	k. A.	k. A.
Preise	Basic einmalig 38,95 US-$, Premium 49,50 US-$ p. a.	15,99 Euro/Monat pro PC, jeder weitere 11,99	auf Anfrage	9,95 Euro/Monat pro PC
Host				
Windows	95/98/ME/XP/Vista/2k/2k3	2k, 2k3	XP, 2k, 2k3	98SE/ME/2000/XP/Vista
Linux	nein	nein	X11	nein
Mac OS	nein	nein	nein	nein
Unix	nein	nein	ja	nein
andere	nein	nein	Terminal Edition	nein
Client (Viewer)				
Browser	für Webbrowser in Arbeit	handelsübliche Webbrowser	Webbrowser	IE7
Web-Java	nein	nein	ja	ja
Windows nativ	95/98/ME/XP/Vista/2k/2k3	95/98/ME/XP	XP, 2k, 2k3	ActiveX
Linux nativ	nein	ab Firefox 2.0, Netscape 7.0, Sun Java	X11	nein
Mac OS nativ	nein	Mac OS 10.3.9, Firefox 1.0, MRJ 2.2.5	nein	nein
Unix nativ	nein	Solaris	nein	nein
Sicherheitstechniken				
Gateway	nein	nein	VPN, WebSecureProxy	–
Nameserver	nein	nein	–	–
Sicherheit	CHAP/RC4(128)	nein	SSL 3, Radius, Smartcard	128 Bit SSL (Zusatz)
SSH	nein	nein	nein	nein
Verschlüsselung	128 Bit RC4	128 Bit AES	AES (128/192/256), 3DES, RC4, Blowfish, CASt, DES, DES_IV32, DES_IV64	k. A.
Passwort-Stärke	k. A.	ja	Länge	k. A.
Authentifizierung	nein	nein	LDAP	–
Zusatzschutz	Host-Passwort	doppeltes Passwort	IPSec (RFC 2401-ff)	–
Ressourcen				
Audio (Voice)	nein	ja	ja	nein
Video	nein	ja	ja	nein
Drucker	nein	ja	ja	nein
lokale Medien	nein	nein	ja	nein
Kompression	ja	ja	ja	k. A.
Dateiübertragung	ja	ja	ja	ja
Drag&Drop	ja	ja	ja	nein
Konferenz (Text)	ja	nein	nein	ja
Logging	ja	k. A.	ja	nein
Monitoring	–	–	–	–
Besonderheiten	–	multiple Monitors, Pocketview	personal Firewall	Handheld, Google Desktop PC-Suche

nahezu unvermeidlichen grafischen Bedienoberflächen hapert es oft an Performance und Synchronisation vor allem zwischen Mausbewegung und -zeiger auf der fernen Oberfläche. Für einfache administrative Aktionen mag das noch erträglich sein, flüssiges Arbeiten ist damit nicht möglich. Einige Firmen bieten umfangreiche Softwarepakete für die Systemverwaltung, mit denen Administratoren die gesamte IT-Umgebung im Blick behalten können und die sich an große Verwaltungs-Frameworks wie Tivoli, HPs Openview und Novells ZENworks anbinden lassen.

Taucht man hinab in die Untiefen der Remote-Control-Verfahren, trifft man auf zwei Strömungen: das Remote Desktop Protocol (RDP) und das Remote Framebuffer Protocol (RFP). Es geht darum, die grafische Darstellung sowie die Interaktion umzulenken und zu kanalisieren. Auf der Open-Source-Seite stehen dafür Tools wie *rdesktop* für RDP und zig Varianten des Virtual Network Computing (VNC) mit dem RFP zur Verfügung. Unter Unix, Linux und BSD fungiert der VNC-Server als eigener X11-Server. Da in der Regel ein X11-Server läuft, belegt VNC den Desktop „:1“. Unter Windows und Mac OS X oder anderen Betriebssystemen nutzt VNC den Desktop „:0“, es sei denn, jemand hat einen X11-Server nachinstalliert. VNC bildet oft die Grundlage für kommerzielle Lösungen und Appliances. Inzwischen haben sich eine Reihe von Ablegern entwickelt, etwa RealVNC, TightVNC oder UltraVNC und andere.

Aber die Frage, welches Protokoll letztlich die Verbindung regelt, tritt

LogMeIn/LoMeIn Pro	NTRconnect Free/Pro	Remote PC	Teamviewer
Logmein Inc.	NTR Global	Pro Softnet Corporation	TeamViewer GmbH
Woburn, Ma./USA	Barcelona, Spanien	Woodland Hills Ca./USA	Uhingen
secure.logmein.com	www.ntrconnect.com	www.remotepc.com	www.teamviewer.com
über Site	über Site	info@remotepc.com	sales@teamviewer.com
Desktop Provider	Remote Desktop	Remote Desktop	Desktop Sharing
mehrsprachig	mehrsprachig	englisch	mehrsprachig
30 Tage oder 120 Min.	30 Tage (Pro-Version)	30 Tage (Full)	für Tests
ja	Free-Version	nein	für Privatanwender
pro PC	pro PC (Free: 2)	pro PC	pro Nutzung
k. A.	per E-Mail	k. A.	Tickets (Browser)
5 PCs für 19,75 US-$ /Monat	6,95 Euro/Monat pro PC	4,95 US-$/Monat pro PC	149 Euro (6 Monate), 499 Euro dauerhaft
ab 98	ab 95	XP, Vista, 2k, 2k3 (>SP4)	ab 98
nein	nein	nein	nein
in Entwicklung	Mac OS X 10.2	nein	nein
nein	nein	nein	nein
nein	nein	nein	nein
IE7	IE7, Netscape, Mozilla, Firefox, Camino und Safari	Webbrowser	Explorer, Firefox
ja	ja	ja	nein
ActiveX	nein	–	ab 98
–	nein	nein	nein
–	nein	nein	nein
–	nein	nein	nein
Pro	Hoster	Hoster	Hoster
–	–	–	–
128/256 Bit SSL, IP-Filter, HMAC-SHA	Passwort, IP-Filter, Zeitgrenzen	128 SSL	RSA/RC4
nein	nein	nein	nein
256 Bit AES (MOOP)	256 Bit AES	128 RC4	–
k. A.	min. 6 Zeichen	min. 4 Zeichen	Sitzungs-ID
HMAC-SHA1	–	–	–
k. A.	Keycard	k. A.	Host-Key
Pro	nein	nein	nein
Pro	nein	nein	nein
Pro	nein	ja	nein
Pro	nein	nein	nein
ja	fest	ja	ja
Pro	ja	ja	nein
Pro	nein	nein	nein
Pro	nein	nein	ja
ja	nein	ja	ja
–	–	–	–
–	Pocket-PC	Remote Data (Zugriff auf Mail und Dateien)	USB-Stick-Version

gegenüber der nach der Sicherheit in den Hintergrund. Schließlich geht es um einen sensiblen Bereich, in dem niemand möchte, dass ihm ein unerkannter Fremder über die Schulter schaut oder Kollegen verwundert und amüsiert dem geisterhaften Treiben auf dem Desktop zuschauen, weil die Remote-Desktop-Software die Anzeige des entfernten Rechners im Büro nicht abgeschaltet hat. Verschlüsselungstechniken sind ein Muss, ein zusätzliches Passwort oder eine spezielle ID bieten zusätzliche Sicherheit. Die Anbieter von Remote-Control-Software werben damit, dass sich der Anwender weder um Firewall-Konfigurationen noch um die Internet-Adressen kümmern muss, da sollten keine offenen Angriffspunkte vorhanden sein.

Bei kurzen Tests fiel auf, dass sich einige Entwickler um die Qualität der Passworte offensichtlich wenig kümmern, während andere restriktiv ein Mindestmaß an Länge und Komplexität verlangen. Außerdem gibt es Unterschiede in der Qualität der Verschlüsselung.

Fazit

Stolperkanten verbergen sich bei den Produkten noch an anderen Stellen. Nur wenige unterstützen auf der Server-Seite Mac OS X oder Unix respektive Linux. Bei den Clients gibt es Einschränkungen, wenn sie ActiveX erfordern. Sie binden sich damit unweigerlich an Windows, oft gar an den Internet Explorer.

Alle Hersteller bieten eine Probeversion zum Test an, NTR Global eine freie Variante, Teamviewer stellt sein Desktop-Sharing privaten Anwendern frei zur Verfügung. Bei den Lizenzen gibt es zwei Modelle: pro Benutzer oder pro PC, gemeint ist der Arbeitsplatzrechner, auf den man zugreifen will. Etwas uneinheitlich verhalten sich die Firmen bei den Preisangaben. Selbst bei denen, die eine deutschsprachige Site betreiben, finden Kunden nur Angaben in US-$. In allen Fällen empfiehlt es sich, das Angebot für die eigene Umgebung zu erproben.

Zwar besticht Remote PC von der Pro Softnet Corporation durch einen günstigen Preis, wirkte aber sogar im LAN ausgesprochen träge. Den mit Abstand höchsten Mietpreis verlangt Teamviewer. Er ist aber der einzige, der mit einer Dauerlizenz zu haben ist, die sich nach wenigen Jahren amortisieren dürfte. In jedem Fall sollte man die Preise vor einer Entscheidung eruieren, denn sie sind gerade in der Branche großen Schwankungen unterworfen.

Aspekte wie Service und Support spielen eine zusätzliche Rolle, die oft nur über Nachfrage zu klären ist. Remote-Controll-Software und speziell die Lösungen für Remote-Desktops gewinnen angesichts der wachsenden Mobilität an Bedeutung, brauchen schon allein deshalb eine gute Unterstützung vonseiten der Hersteller. (rh)

Literatur

[1] Dieter Michel; Dick und Dünn; Applix Anyware und Corel Office for Java; *iX* 7/1997, S. 58

[2] Gerhard Versteegen; Outsourcing; Neuer Anlauf; Im Detail: „Software as a Service“; *iX* 8/2007, S. 101

[3] Axel Urbanski; Fernwartung; Allein zu Haus; KVM over IP: zehn Geräte im Vergleich; *iX* 3/2005, S. 48

[4] Ralph Hülsenbusch; Remote Desktop; Tischleindeckdich; Der Arbeitsplatz im Netz – von überall erreichbar; *iX* 10/2006, S. 42

Datentransport in versteckten Übertragungskanälen



Versteckspiel

Martin Kappes, Andreas Renner

TCP/IP-Netze transportieren Unmengen an Daten. Nicht alle müssen sich an den dafür vorgesehenen Stellen befinden: So können Header-Felder mehr Informationen enthalten, als auf den ersten Blick erkennbar ist.

Unzählige Legenden ranken sich darum, wie Geheimdienstagenten und ihre Informanten in Zeiten des kalten Kriegs wichtige Nachrichten aus dem Land des Gegners schaffen und dabei Leib und Leben riskieren mussten. Dank des Internet und kryptografischer Verfahren scheint es auf den ersten Blick inzwischen deutlich leichter zu sein, vertrauliche Nachrichten geschützt zu übermitteln.

Das Verschlüsseln von Daten kann zwar verhindern, dass Unbefugte die geschützten Informationen nutzen, doch es hilft kaum dabei, Nachrichten unbemerkt zu versenden. Denn wenn auch der Inhalt unsichtbar bleibt, lässt sich dennoch nicht verheimlichen, dass Information fließt und eine Kommunikation stattfindet. Es ist ungefähr so, als wenn man versuchte, etwas durch den Zoll zu schmuggeln, indem man es in einem Tresor transportiert.

Ein Beispiel aus der Welt der Informatik ist das Kommunikationsverhalten von Malware, das gerade zur Entdeckung solch unerwünschter Programme führen kann. Einige Schadprogramme kontaktieren andere Rechner über das Internet, etwa in Bot-Netzen. Selbst wenn diese Kommunikation verschlüsselt abläuft oder ihr Inhalt nicht weiter beobachtet wird, kann der ungewöhnliche Verkehr zwischen dem befallenen Rechner und den kontaktierten Maschinen doch auffallen und so zur Entdeckung der Schadsoftware führen, auch wenn man nicht genau nachvollziehen kann, welche Information die Malware weitergeleitet hat. Allein die Kenntnis von Verbindungsdaten kann ein wichtiges Indiz für bestimmte Vorgänge sein.

Zwischen den Zeilen übertragen

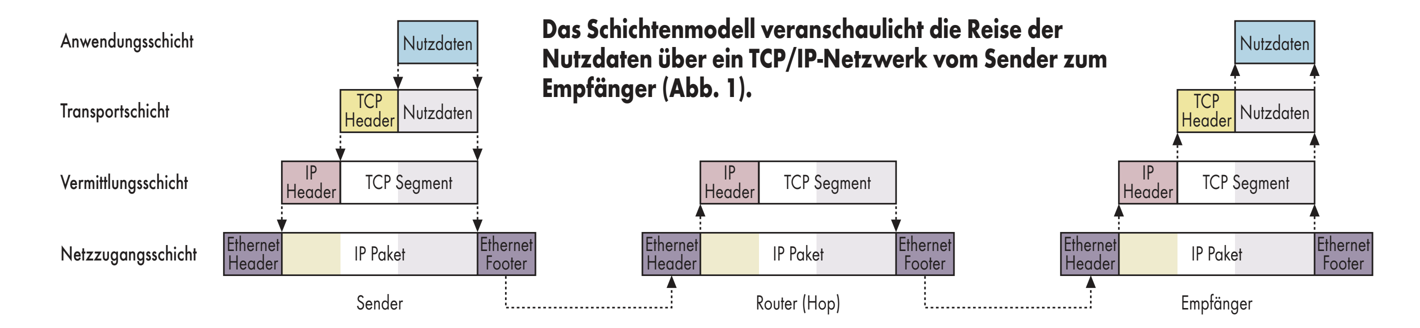
Mit der Frage, wie man unbemerkt Informationen übermitteln kann, beispielsweise indem man sie in einer Nachricht mit scheinbar harmlosem Inhalt versteckt, beschäftigt sich die Steganografie. Klassisches Beispiel eines steganografischen Verfahrens ist die Verwendung unsichtbarer Geheimtinte zum Verstecken einer Botschaft in einem scheinbar harmlosen Brief. Mit Spezialtinte, die erst durch eine Sonderbehandlung (Schwärzen mit Ruß et cetera) sichtbar wird, kann der Absender in dem Brief eine geheime Botschaft verstecken.

In der elektronischen Datenverarbeitung ist die Steganografie zu neuen Ehren gekommen. Eine der bekanntesten Anwendungen ist das Verstecken von Botschaften in Bildern oder Audiodateien. Bestimmte Bildformate enthalten für jedes Pixel eine sehr detaillierte Farbinformation. Geringfügige Veränderungen der Farbinformation fallen einem menschlichen Betrachter nicht auf, sodass man das letzte Bit der Farbinformation zum Verstecken von Nachrichten nutzen kann. In einem unkomprimierten Bild mit 1280 × 1024 Pixeln lassen sich auf diese Weise beachtliche 160 KByte verstecken.

Diese Vorgehensweise bildet auch den Grundstein für digitale Wasserzeichen. In bestimmten Teilen eines Bildes befinden sich Informationen, die für einen Betrachter nicht wahrnehmbar sind. Digitale Wasserzeichen lassen sich etwa zur Nachverfolgung von Bildquellen einsetzen. Natürlich kann eine steganografisch übertragene Nachricht zusätzlich verschlüsselt werden.

Netzwerk- oder Datensicherheit

Steganografie ist nicht auf das Verstecken von Informationen in Anwendungsdaten beschränkt, sondern kann auch beim Transport von Daten über das Internet zum Einsatz kommen [2-4]. Bevor ein Datenpaket einen Rechner verlässt und einen anderen erreicht, beschäftigt es nacheinander eine ganze Reihe von Netzwerkprotokollen (Abb. 1).



Das Schichtenmodell veranschaulicht die Reise der Nutzdaten über ein TCP/IP-Netzwerk vom Sender zum Empfänger (Abb. 1).

Die für das Verstecken von Daten interessanten Schichten im Internet-Protokollstapel sind die Datenverbindungsschicht, die Netzwerkschicht (IP) und die Transportschicht, auf der entweder das Transmission Control Protocol (TCP) oder das User Datagram Protocol (UDP) zum Einsatz kommt. Die Header-Daten der Transportprotokolle werden normalerweise ausschließlich von den beiden kommunizierenden Endsystemen geschrieben oder gelesen.

Beim Versenden von Daten werden die Schichten von oben nach unten durchlaufen, und jedes verwendete Protokoll hängt jeweils notwendige Verwaltungs- und Steuerungsinformationen in Form eines Headers oder Trailers an die Nutzdaten an. Auf der Empfängerseite werden die Schichten in umgekehrter Reihenfolge von unten nach oben durchlaufen und dabei die Header wieder entfernt, bis nur noch die ursprünglich versendeten Nutzdaten übrig bleiben [1].

Zur freien Verwendung

Header-Daten benötigen die Protokolle dafür, ihre jeweilige Aufgabe erfüllen zu können. Da die Protokolle der verschiedenen Schichten ganz unterschiedliche Aufgaben übernehmen, können sich die in den einzelnen Feldern des Headers enthaltenen Verwaltungsinformationen in Bezug auf Art, Inhalt und Darstellung von Protokoll zu Protokoll stark voneinander unterscheiden.

IP-Header enthalten unter anderem die Quell- und Zieladresse des Datenpakets (Abb. 2). Doch es gibt auch Header-Felder, die unter bestimmten Umständen vollkommen ignoriert werden oder solche, die nur einen geringen Einfluss auf die Paketbehandlung haben. Nicht alle Header-Felder spielen für die Behandlung der Pakete durch das jeweilige Protokoll eine Rolle, und so lassen sich einige davon für andere als die vorgesehenen Zwecke nutzen.

Ein Beispiel im IP-Header ist das 16 Bit große Feld „IP-Identification“, kurz IP-ID. Es dient laut RFC 791 dazu, im Falle einer Fragmentierung die Teile den ursprünglichen Paketen zuzuordnen. Dazu muss der Absender die IP-ID so wählen, dass sie gemeinsam mit Quell- und Zieladresse des Pakets eine Verwechslung mit Fragmenten anderer Pakete ausschließt. Man kann dies aber auch sicherstellen, ohne dieses Feld voll auszunutzen. Zudem wird die IP-Fragmentierung heutzutage weitgehend mittels Path-MTU-Discovery vermieden. Dementsprechend ist in fast allen IP-Paketen das „Don’t fragment“-Bit gesetzt, das die Zerlegung des betreffenden Pakets verbietet. Das daher heute oft nicht mehr relevante IP-ID-Feld eignet sich wunderbar dazu, Daten versteckt zu transportieren – 2 Byte pro IP-Paket.

Es gibt verschiedene Szenarien, die Manipulation von Header-Feldern zur verdeckten Informationsübermittlung zu nutzen:

Gesetzt den Fall, Alice möchte sich mit ihrem alten Bekannten Dave in einem Restaurant treffen und dafür einen Zeitpunkt vereinbaren. Hiervon soll Alices Mann Bob aber keinesfalls etwas erfahren, denn er neigt zu rasender Eifersucht. Deshalb liest Bob in Alice und Bobs gemeinsamen Heimnetzwerk unter Missachtung aller strafrechtlich relevanten Bestimmungen alle E-Mails und Instant Messages mit, die Alice versendet. Alice weiß das und verwirft deshalb sofort die Idee, mit Dave einfach verschlüsselt zu kommunizieren, da dies Bob nur noch misstrauischer machen würde.

Sie entschließt sich stattdessen, einen eigenen Webserver zu betreiben und einigen Freunden, unter anderem Dave, dessen Adresse zu geben. Immer dann, wenn eine Anfrage von Daves IP-Adresse kommt, versteckt Alice ein paar Byte in den Antwortpaketen. Ebenso kann Dave in den Anfragen unauffällig Informationen unterbringen, sodass die beiden auf diese Weise einen Dialog führen können. Treffpunkt und Zeitpunkt lassen sich mit wenigen Paketen vereinbaren, ohne dass Bob Verdacht schöpft.

In einem zweiten Szenario hat sich Bob auf seinem Rechner einen „Trojaner“ von Eve eingefangen. Das Überwachungsprogramm soll Informationen von Bobs PC möglichst unauffällig nach draußen transportieren (Abb. 3). Eve hat zudem sichergestellt, dass Pakete an bestimmte IP-Adressen (oder sogar alle Pakete), die Bob über seinen Internet-Provider versendet und empfängt, über einen Computer unter Eves Kontrolle laufen. So kann sie das Header-Feld dafür nutzen, Informationen von Bobs Computer unbemerkt auszuschleusen und dem von ihr installierten Trojaner Instruktionen zuzusenden.

Je einfacher, desto besser

Steganografie mithilfe der Header von Netzprotokollen bietet einige wesentliche Vorteile gegenüber dem Verstecken von Daten auf der Anwendungsschicht. Gerade im zweiten Szenario kann ein Überwachungsprogramm die Pakete während deren Bearbeitung durch das System manipulieren und die eingehenden Pakete ebenfalls auswerten. Das Einfügen und Auslesen der versteckten Daten erfordert keine Kenntnisse oder Annahmen über den

iX-TRACT

- Die Internet-Protokolle bieten in nicht benötigen Teilen der Datenpakete zahlreiche Optionen zum Verstecken von Informationen.
- Gut zehn Prozent der Nutzdaten lassen sich über verdeckte Kanäle transportieren, die normale Anwendungen nicht erfassen.
- Vorsorgemaßnahmen in der eigenen Netztopologie können verhindern, dass versteckte Daten das eigene Netz verlassen.

Charakter der zugrunde liegenden Kommunikation. Dies ermöglicht eine vergleichsweise einfache Realisierung, bei verdeckt arbeitenden Programmen besonders wichtig.

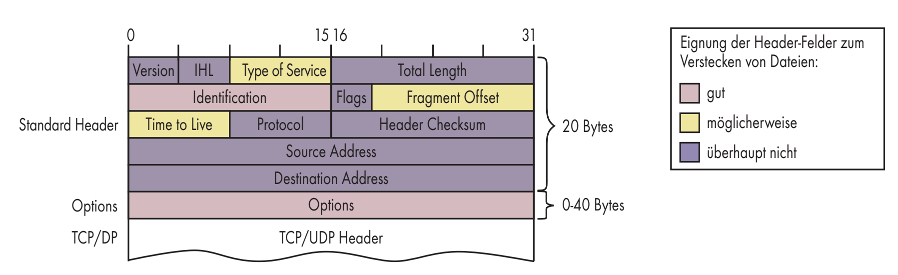
Dazu kommt, dass sich auf diese Art dauerhaft und stetig Daten transportieren lassen, da ein Arbeitsplatzrechner üblicherweise ständig IP-Pakete versendet – sei es zum Abrufen der E-Mails, von Webseiten oder durch Peer-to-Peer-Aktivität.

Eine technische Umsetzung solcher Verfahren ist beispielsweise unter Linux denkbar einfach. Die Kernel-Komponente der Linux-Firewall „Netfilter“ stellt eine Reihe sogenannter „Hooks“ bereit, die Netzwerkpakete zwecks Manipulation abfangen können.

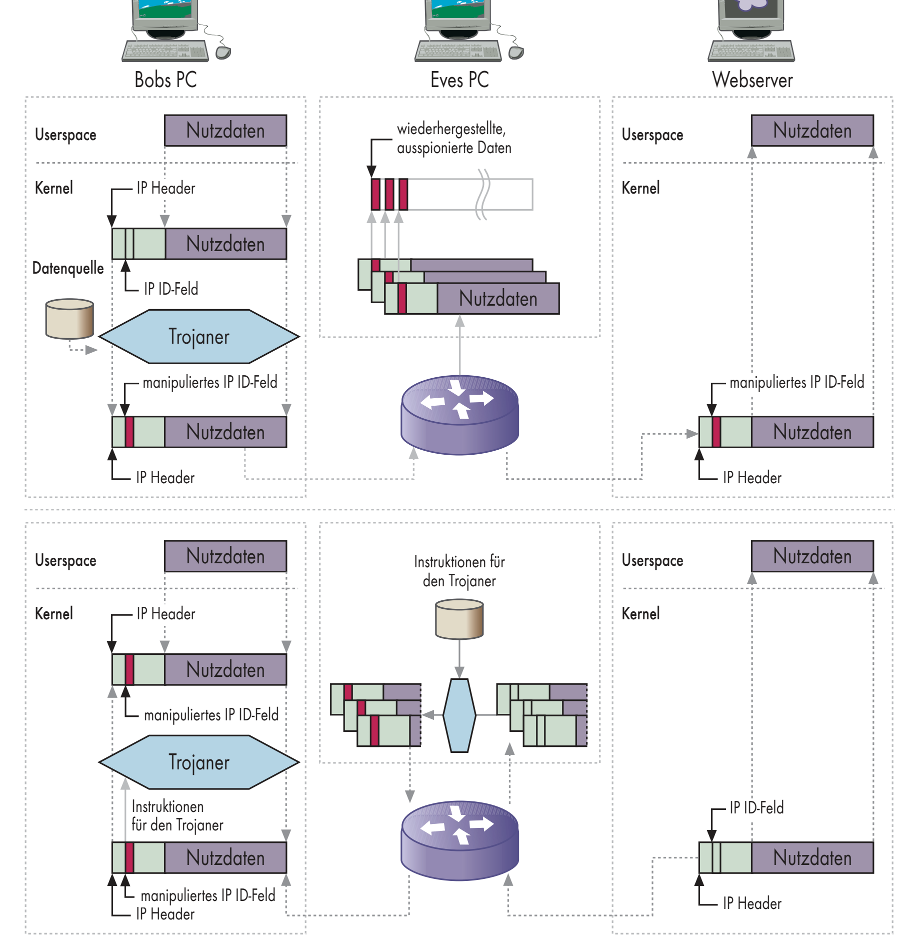
In einem Kernel-Modul kann man dem Netfilter-Framework eine Callback-Funktion übergeben, die immer dann aufgerufen wird, wenn ein interessantes Datenpaket den Hook passiert. In einer Datenstruktur bestimmt man den Namen der Callback-Funktion und an welchen Paketen man Interesse hat.

Bei jedem Aufruf wird der Callback-Funktion der „Socket Buffer“ (skb) übergeben, der das Paket selbst sowie Metainformationen wie das ausgehende Netzwerk-Device enthält. In diesem Socket Buffer lassen sich die IP-Header-Felder einfach durch Zuweisung ändern. Nach jeder Änderung muss die Prüfsumme (checksum) erneut berechnet werden, da sonst der nächste Router das Paket verwirft. Nach dem Rücksprung aus der Callback-Funktion läuft das Paket normal weiter, in diesem Fall also über das ausgehende Device.

Ein Kernelmodul, das die hier beschriebene Funktion umsetzt, umfasst weniger als 500 Zeilen C-Code. Die zu versendenden Daten sind beliebig wählbar. Als Datenquellen wären beispielsweise ein „Character Device“, Dateien vom lokalen Dateisystem oder auch die Tastatureingaben des Benutzers („Keylogger“) denkbar.



Die Felder des IP-Headers und ihre Eignung zum Verstecken von Daten (Abb. 2)



Oben: Eve erhält die Daten, die der Trojaner auf Bobs PC sammelt und im IP-Header versteckt. Unten: Eve schleust Instruktionen für ihren Trojaner auf Bobs PC in den Datenverkehr des Webservers ein (Abb. 3).

Weite und zu weite Felder

Außer der IP-ID eignen sich weitere Header-Felder zum Verstecken von Daten, insbesondere im Rahmen von TCP. Infrage kommen prinzipiell alle Felder, deren Veränderungen die Semantik nicht merklich beeinflussen, was zu einer Beeinträchtigung der Netzwerkkommunikation führen könnte. Insbesondere der 2 Byte lange TCP-Urgent-Pointer bietet sich an, der auf das Ende vorzugsweise zu bearbeitender Daten innerhalb der Nutzlast zeigt. Ihn interpretieren Netz-Devices nur bei gesetztem URG-Flag. Im Gegensatz zur üblichen Vorgehensweise, ungenutzte Felder auf Null zu setzen, ist der Wert des Urgent Pointer bei nicht gesetztem URG-Flag nicht spezifiziert. Damit lassen sich diese 2 Byte sogar RFC-konform für beliebige Daten nutzen.

Für das subtile Unterbringen größerer Datenmengen in einem Paket bieten sich sogenannte Header-Optionen an, die sowohl IP als auch TCP vorsehen (Abb. 4). Optionen müssen, wie der Name schon andeutet, nicht vorkommen, bieten aber zusätzlichen Platz zum Verstecken von Daten. Zu den bekannteren IP-Optionen zählt „Record Route“, die einen Bereich im Header freihält, in den die Hops auf dem Weg ihre IP-Adresse eintragen. Anstelle von IP-Adressen kann man natürlich auch eine Nachricht in dem Freiraum verstecken. Netzwerkanalyse-Tools würden den Inhalt als IP-Adressen interpretieren, was das Entdecken der Nachricht erschwert.

Man kann sogar noch einen Schritt weiter gehen: TCP kennt zwei spezielle,

ein Byte lange Optionen: „No Operation“ (NOP) und „End of Option List“ (EOL). NOPs dienen der Anordnung (Padding), da die Länge der Optionen einem Vielfachen von 4 Byte entsprechen muss. Auf das EOL-Byte folgende Bytes im TCP-Header werden nicht mehr interpretiert. So können fast alle ungenutzten Bytes der maximal 40 Byte großen TCP-Header-Optionen dem Verstecken von Daten dienen. Dafür sind lediglich ein NOP- und ein EOL-Byte an die eventuell bereits vorhandenen Optionen anzufügen. Die restlichen Bytes, die die Differenz zur maximalen Optionslänge bilden, stehen so zur freien Verfügung, da ein TCP/IP-Stack sie ignoriert.

Innerhalb eines LAN-Segments lassen sich sogar deutlich größere Datenmengen unauffällig mitsenden. Der IP-Header enthält ein Feld namens „Total Length“, das die Gesamtlänge des IP-Pakets angibt. Doch die dort angegebene Länge muss nicht mit der tatsächlich auf der Datenverbindungsschicht übertragenen Nutzlast übereinstimmen, sondern kann kleiner sein. Genau dieser Platz lässt sich im Frame des Datenverbindungsschicht-Protokolls dafür nutzen, Informationen zu verstecken.

In lokalen Netzen kommt üblicherweise Ethernet zum Einsatz, das eine maximale Frame-Größe (MTU) von 1500 Byte zulässt. Die Differenz zwischen der MTU und der Größe des IP-Pakets lässt sich so zum Verstecken von Daten verwenden. Da viele der gesendeten IP-Pakete verhältnismäßig klein sind (etwa TCP-ACKs), kann diese Methode zu einem beachtlichen Datendurchsatz führen. Da der IP-Stack alle hinter den im „Total Length“-Feld angegebenen Daten ignoriert, beeinträchtigt diese Methode die Kommunikation auf IP-Ebene nicht. Allerdings hat dies auch zur Folge, dass der erste Router die so versteckten Daten ebenfalls ignoriert und daher vor dem Weiterleiten entfernt. Auf diese Weise versteckte Informationen sind daher nur im jeweiligen Netzsegment verfügbar.

Modem-Durchsatz versteckt übertragen

Den höchsten Durchsatz erhält, wer die Methoden zur heimlichen Unterbringung der Daten miteinander kombiniert. Zur experimentellen Ermittlung typischer Werte für die Größe der in einem Paket tatsächlich maximal versteckbaren Datenmenge diente ein Linux-Desktop-System, auf dem ein Bittorrent-Client lief und das E-Mails sowie Webseiten abrief. Die Daten wurden soweit möglich in der IP-ID, dem TCP Urgent Pointer und in den TCP-Optionen untergebracht.

Im Durchschnitt ließen sich auf diese Weise 30 Byte pro Paket versenden, immerhin etwa 11 % der Gesamtdatenmenge. So lässt sich das Äquivalent zum guten, alten 14,4-kbps-Modem in einem zu zwei Dritteln ausgelasteten Upstream eines typischen 2-Mbps-DSL-Anschlusses unterbringen.

So schön das Unterbringen von geheimen Daten in den Header-Feldern auch ist, wirklich unauffällig bleibt der Transport nur, wenn die Änderung der Header-Daten keine unerwünschten Auswirkungen auf die Kommunikation hat. Änderungen an den IP-Adressen oder TCP-Portnummern scheiden somit aus, denn dann würden die Pakete ihren Bestimmungsort nicht mehr erreichen. Das Manipulieren der Felder „TCP Sequence“ und „TCP Acknowledgement Number“ würde zu unnötigerweise wiederholten Übertragungen führen und damit den Durchsatz reduzieren. Das Feld „Time to Live“ (TTL) wird von jedem Router auf dem Weg zum Ziel um eins dekrementiert, und die Anzahl der Router auf dem Weg kann für jedes Paket anders sein.

Nicht alle Header-Felder, die auf den ersten Blick geeignet erscheinen, überstehen ihre Reise unbeschadet. Wendet man etwa den „Trick“ mit den TCP-Optionen auf IP an, kann es passieren, dass der empfangende IP-Stack alle Bytes hinter der Markierung „End of Option List“ auf Null setzt. Generell sollte man darauf verzichten, IP-Optionen zu verwenden. Selbst Pakete mit den „harmlosen“ Optionen „Record Route“ und „Internet Timestamp“ kommen meist nicht ans Ziel, da sie entweder vom eigenen Provider oder einer Firewall des Empfängers ausgefiltert werden.

Alte Verstecke in neuen Protokollen

In den nächsten Jahren wird die gegenwärtig eingesetzte IP-Version 4 nach

und nach durch IPv6 abgelöst. IPv6 scheint für das Verstecken von Informationen im Header auf den ersten Blick wenige Möglichkeiten zu bieten, da sich die Anzahl der Felder im Vergleich zu Version 4 deutlich verringert hat. Erreicht wurde dies durch eine Auslagerung nicht ständig benötigter Header-Felder in sogenannte Extension-Header, von denen mehrere in einem Paket auftreten können. Einige dieser Extension-Header bieten ähnliche Verstecke wie IPv4 [5].

Von den Feldern im eigentlichen Header kommt vor allen Dingen das im Vergleich zu IPv4 neu hinzugekommene Feld Flowlabel für den verdeckten Datentransport infrage. Es dient eigentlich dem schnelleren Bearbeiten zusammengehöriger Pakete. Da Router jedoch nicht zuvor zugewiesene Flowlabel ignorieren, wäre ein Füllen mit anderen Daten denkbar.

Unter den Extension-Headern gibt es einen, der die Fragmentierung von Paketen erlaubt und ein Feld enthält, dessen Verwendung in etwa der IP-ID aus IPv4 entspricht. Ein weiterer ist der Destination Options Header. Er bildet die bereits bekannten IPv4-Optionen ab und hat den zusätzlichen Vorteil, dass er unterwegs weder interpretiert noch verändert werden darf. Insgesamt finden also die Freunde des verdeckten Informationstransports auch mit IPv6 diverse Verstecke.

Spion vs. Spion

Steganografische Verfahren lassen sich aber mit statistischen Methoden oft einfach entdecken, etwa da ein bestimmtes Merkmal plötzlich eine veränderte Verteilung aufweist. Wirksamer noch als der Versuch, solche Manipulationen nachträglich zu entdecken, ist jedoch deren gezielte Verhinderung.

Wer Steganografie in seinem Netz nicht dulden möchte, kann die Anwendung der genannten Methoden deutlich erschweren. Am gründlichsten gegen heimlich transportierte Informationen auf den unteren Schichten des Netzwerks wirkt ein Application Level Gateway (ALG), etwa ein Web-Proxy. Die manipulierten Pakete gelangen nur bis dorthin, bleiben also im eigenen Netz, denn das ALG erstellt selbst neue Pakete auf dem ausgehenden Interface.

Aufspüren ist möglich

Ist der Verzicht auf IP-Routing keine Option, bleibt immer noch der Einsatz restriktiver Firewall-Regeln. So kann eine Firewall den TCP-Urgent-Pointer immer auf Null setzen, wenn das URG Flag nicht gesetzt ist, ohne die Nutzer hinter der Firewall einzuschränken. Ebenso können die IP-IDs nicht fragmentierter Pakete grundsätzlich mit Null überschrieben, TCP-Optionen hinter dem EOL-Byte auf Null gesetzt und unbekannte Optionen ganz entfernt werden.

Das Aufspüren heimlich transportierter Daten in standardisierten TCP-Optionen ist deutlich schwieriger und nur durch eine Analyse der Optionswerte möglich. Besonders subtil ist das Verstecken von Informationen in der Initial Sequence Number (ISN) bei TCP-Verbindungen, die beim Aufbau der Verbindung zufällig entsteht. Allerdings würde die Umsetzung einen tieferen Eingriff in den Kernel erfordern und der Datendurchsatz wäre extrem gering, da sich maximal 4 Byte pro TCP-Verbindung transportieren lassen. Als Gegenmaßnahme könnte man durch die Perimeter-Firewall die ISNs aller TCP-Verbindungen um einen zufälligen Offset verschieben. Dies würde allerdings hohe Anforderungen an die Firewall stellen, die „stateful“ sein und alle TCP-Segmente verändern müsste. Generell muss ein Netzadministrator zwischen der Aufspürbarkeit der versteckten Daten und dem erzielbaren Durchsatz abwägen.

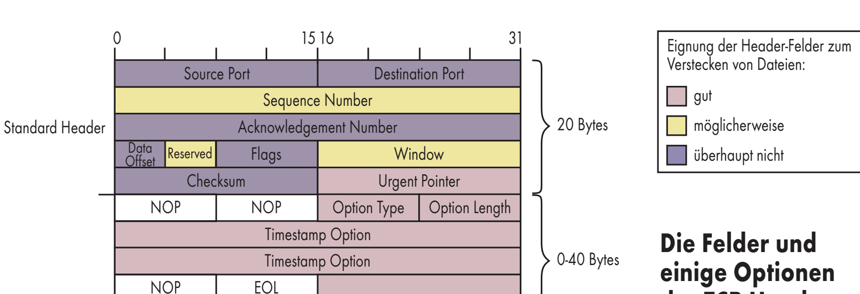
Mittels Steganografie bieten sich subtile Möglichkeiten, durch die Verwendung nicht benötigter Header-Felder in Protokollen Informationen aus einem Rechner auszuschleusen, die insbesondere Schadsoftware verhältnismäßig einfach nutzen kann. Solche Ansätze sind schon seit einiger Zeit bekannt, aber bisher vor allem von akademischem Interesse [2-4]. Die zunehmende Überwachung und Zensur des Internet in manchen Ländern auf der einen und die verbesserte Abwehr gegen Schadprogramme und Spionage andererseits machen es aber durchaus wahrscheinlich, dass Steganografie in Datennetzen in Zukunft an Bedeutung gewinnen könnte. Dabei kann Steganografie – wie die Kryptografie – sowohl zu kriminellen als auch rechtschaffenen Zwecken eingesetzt werden.

PROF. DR. MARTIN KAPPES

ist Professor für Informatik, insbesondere Rechnernetze und Betriebssysteme, an der Fachhochschule Frankfurt am Main. Seine Arbeitsschwerpunkte liegen im Bereich Netzwerk- und Systemsicherheit.

ANDREAS RENNER

studiert an der Fachhochschule Frankfurt am Main Informatik mit Schwerpunkt Rechnernetze.



Die Felder und einige Optionen des TCP-Headers und ihre Eignung zum Verstecken von Daten (Abb. 4)

Literatur

[1] Martin Kappes; Netzwerk- und Datensicherheit; Teubner; 2007
[2] Deepa Kundur, Kamran Ahsan; Practical Internet Steganography: Data Hiding in IP; www.ece.tamu.edu/~deepa/pdf/txsecwrksh03.pdf
[3] C.H. Rowland; Covert channels in the TCP/IP protocol suite; Tech. Rep. 5, First Monday, 1997; www.firstmonday.org/Issues/issue2_5/rowland/
[4] S.J. Murdoch and S. Lewis; Embedding Covert Channels into TCP/IP; 2005; www.cl.cam.ac.uk/~sjm217/ papers/ih05coverttcp.pdf
[5] Norka B. Lucena, Grzegorz Lewandowski, Steve J. Chapin; Covert Channels in IPv6; Privacy Enhancing Technologies, Springer Berlin/Heidelberg, 2006

IBMs Midrange-Betriebssystem i5/OS V6R1

Eine eigene Liga

Berthold Wesseler

Die objektbasierte Struktur und die damit verbundenen Eigenarten sind der Grund, warum die AS/400 mit OS/400 unter dem neuen Namen System i unter i5/OS immer noch gefragt ist. Mit der neuen Version V6R1 rückt es näher an die Unix-Systeme aus dem gleichen Hause heran.

Am 21. März will IBM die im vergangenen Jahr avisierte neue Version des Betriebssystems i5/OS V6R1 für die Serverbaureihe System i auf den Markt bringen. Neben zahlreichen Erweiterungen des Funktionsumfangs und der Verbesserung der Performance fällt vor allem die Unterstützung für die neuen Power-Blades JS22 ins Auge: Erstmals lässt sich i5/OS auf einer anderen Rechnerfamilie als dem System i einsetzen, und zwar nicht nur auf den Modellen mit dem jüngsten Power6, sondern auch auf den Vorgängern mit Power5 und Power5+. Umgekehrt versetzt IBM die aktuelle Release i5/OS V5R4 per Patches in die Lage, auf Power6-Rechnern zu laufen. Unterstützung durch i5/OS V6R1 finden zunächst die Power6-Blades JS22 im Bladecenter H und später im Verlauf des Jahres im für Filialen und kleinere Unternehmen erdachte Bladecenter S.

Um i5/OS auf den Power6-Blades lauffähig zu bekommen, hat IBM tief in die Trickkiste gegriffen: Voraussetzung ist der Virtual I/O Server (VIOS). Der wiederum bildet den I/O-Layer des System-p-Hypervisors namens Power VM, unter dem Namen Advanced Power Virtualization der Power5+-Generation unter AIX und Linux entsprungen. VIOS erlaubt es mehreren logischen System-p-Partitionen, gemeinsam auf SCSI-Geräte oder Ethernet-Ports zuzugreifen. Mit i5/OS V5R1 bekommt der Virtual I/O Server nun einen neuen Gast – allerdings nur auf den Power6-Servern.

Immer zu Diensten

Auf der JS22-Blade – oder dem Bladecenter – muss man zuvor eine VIOS-Partition einrichten. Sie stellt den i5/OS-Partitionen die angeschlossenen Speicherressourcen zur Verfügung. Begründet ist dieser Umweg darin, dass die für die Blades notwendigen Treiber bereits virtualisiert sind und IBM von einer Re-Portierung zum nativen Betriebssystem Abstand genommen hat. Auf dem System i ist eine solche Konstruktion vor allem dann von Vorteil, wenn man eigene i5/OS-Partitionen zum Testen von i5/OS-Anwendungen benötigt, da man auf die Anschaffung und Installation separater Hardware verzichten kann.

Bereits auf die Blades angepasst ist der Integrated Virtualization Manager (IVM), der nun der traditionellen Hardware Management Console (HMC) zur Seite steht. Der IVM kann nicht nur die i5/OS-Partitionen steuern und verwalten, die über den VIOS an die Blade angeschlossene Speicherhardware nutzen, sondern auch die VIOS-Partition selbst managen. Beispielsweise kann man mit dem IVM Partitionen erzeugen oder entfernen. Als Anhaltspunkt für die Performance des i5/OS auf der JS22-Blade gibt IBM übrigens 11 040 CPW (Commercial Processing Workload) an; ein System-i-Einstiegsmodell der Baureihe 525 mit Power5+-Prozessor kommt auf 7100 dieser IBM-typischen Leistungseinheiten.

Schon früher konnte das System i übrigens als virtuelles Storage Area Network (SAN) AIX- und Linux-Server bedienen – und über eine iSCSI-Verbindung auch andere. Schon im September 2007 ist bei der Speichervirtualisierung für Windows- oder Blade-Server die Unterstützung für den ESX-Server von VMware hinzugekommen, sodass die darunter gehoste-

ten Gastsysteme die Speicherressourcen des System i nutzen können.

Ebenfalls neu sind die „Storage Space Snapshots“, über die sich sogenannte Hot Backups – also Datensicherungen im laufenden Betrieb – virtueller i5/OS-, AIX-, Linux-, VMware- und Windows-Server erstellen lassen. Spareffekte bei größeren System-i-Anwendungen bringt die neue Option der Shared Processor Pools. Mit ihr lassen sich mehrere Partitionen mit dynamischen Prozessorkapazitäten zu einer Gruppe zusammenfassen und dieser eine gemeinsame Obergrenze für die Prozessorzahl zuordnen. Das senkt die Softwarelizenzkosten, die sich bisher aus der Summe der Maximalkapazitäten der einzelnen Partitionen berechnen. IBM bietet dieses Feature auch für die aktuelle Release V5R4 an, allerdings nur auf den neuen Power6-Maschinen.

Direkt ins Betriebssystem integriert hat Big Blue den Verschlüsselungsstandard AES. Damit lassen sich zum einen Backups – mit der hauseigenen Datensicherungssoftware „Backup Recovery and Media Services“ (BRMS) –, zum anderen Daten auf Festplatten – in einem sogenannten Auxiliary Storage Pool (ASP) – verschlüsseln. Nutzen lässt sich die AES-Implementierung allerdings nur über die kostenpflichtigen Optionen 44 für die verschlüsselte Bandsicherung und 45 für die Verschlüsselung der ASPs. Da für die Verschlüsselung kein eigener Koprozessor zur Verfügung steht, darf man auf die Performance in der Praxis gespannt sein.

Zudem versieht das System alle Programme automatisch mit einer digitalen Signatur. Das soll ihre Authentizität garantieren und verhindern, dass Programme unterhalb des Technology Independant Machine Interface (TIMI) des Systems operieren können. Für bestehende Programme, die das TIMI nutzen, steht deshalb beim Umzug auf die Release V6R1 eine Konvertierung an, für die IBM eigene Tools mitliefert.

Keine Chance für Angreifer

Erweitert hat IBM die Intrusion Detection and Prevention. Sie befähigt das System, in einem von i5/OS kontrollierten Netz Clients ausfindig zu machen, die eine Denial-of-Service-Attacke gestartet haben. Außerdem kann es automatisch Benachrichtigungen per E-Mail oder Pager versenden, falls es Risiken entdeckt oder wenn kritische IT-Komponenten nicht ordnungsgemäß funktionieren. Überarbeitet hat Big Blue auch das Event-Logging. Die neue Intrusion-Prevention-Technik hat IBM kürzlich zum Patent angemeldet und jetzt erstmals auf den Markt gebracht; die anderen Server-Plattformen sollen später ebenfalls damit ausgerüstet werden.

Weitere Neuerungen sind der iCluster und der High Availability Solutions Manager (HASM). iCluster stammt aus der Übernahme des kanadischen Softwarehauses Datamirror im vergangenen Jahr und dient zur asynchronen Replikation der Daten auf einen Backup-Server. HASM dagegen ist eine Option für die hardwarebasierte Replikation und das Clustering im Zuge des sogenannten Cross-Site Mirroring (XSM) in Hochverfügbarkeitsumgebungen und zur Katastrophenvorsorge.

Für das webgestützte Multisystem-Management wird i5/OS V6R1 den IBM Systems Director Navigator for i5/OS nutzen. Er soll das bisherige Administrationswerkzeug, den i5/OS Navigator, in der nächsten Betriebssystem-Release ablösen. Erklärtes Ziel ist es, die bisherigen Managementfunktionen zu erweitern, um gemischte IT-Umgebungen besser unterstützen zu können. Der Systems Director Navigator for i5/OS ist ein webbasiertes Administrations-Interface, das den nun integrierten Web-Application-Server nutzt und mit über 300 vordefinierten Management-Tasks ausgestattet ist. Künftige Versionen sollen mehrere unterschiedliche Betriebssystemumgebungen in einem Browser darstellen können. Bereits heute unterstützt der Server die in der Release V6R1 hinzugekommenen Systemfunktionen wie HASM oder den Performance Data Investigator, der der Darstellung und Analyse des Systemleistungsverhaltens dient.

iX-TRACT

- Mit i5/OS V6R1 stellt IBM im März die neue Generation seines Midrange-Betriebssystems vor.
- Zu den großen und kleinen Erweiterungen gesellt sich die Fähigkeit, auf der Power6-Blade zu laufen.
- Dazu ist aber der Virtual IO Server notwendig: i5/OS agiert erstmals selbst als Gast.

Der neue Web-Application-Server soll die Einführung von Java-Applikationen erleichtern, die JSF, JSP und Servlets nutzen – und weniger Systemressourcen und Verwaltungsaufwand als bisher benötigen. Hinzu gesellen sich eine performantere 64-Bit-Implementierung der Java Virtual Machine, die die Java-Performance um 70 bis 80 % erhöhen soll, und ein Enterprise Service Bus (ESB) auf Betriebssystemebene.

Zu diesen grundlegenden Erweiterungen kommen Verbesserungen im Detail: Beispielsweise hat IBM die integrierte SQL-Datenbank deutlich erweitert, etwa um die Möglichkeit der Textabfrage. Zur PC-Anbindung dient nun System i Access V6R1, erhältlich für Linux, für Windows und als Webvariante, zu deren Verbesserungen ein optimierter Vista-Support durch die Terminal-Emulation PC5250, IPv6-Support und Erweiterungen beim Datenbankzugriff per ODBC gehören.

Zukunft für RPG

Last but not least soll das Integrated Language Environment (ILE) eine integrierte Webservices-Umgebung erhalten, inklusive Schnittstellen für ILE-Programme sowie einer Laufzeitumgebung für Webservices, die auf vorhandene Cobol- und RPG-Programme auf dem System i zugreifen können. Auch künftig will IBM in die Weiterentwicklung der Programmiersprache RPG investieren, sei es in die Integration neuer Techniken wie Webservices, die sich aus RPG heraus nutzen lassen, oder in Compiler-Erweiterungen für Multithreading und die Unterstützung lokaler Dateien, was die parallele Nutzung vorhandener RPG-Programme durch Webservices erleichtern soll.

Dass Big Blue die Entwicklung der System i-Compiler und Software-Entwicklungswerkzeuge in den Geschäftsbereich Rational verlagert hat, soll vor allem die Integration und Synergie von Produkten wie dem Websphere Development Studio Client (WDSC) mit anderen Rational-Tools verbessern, heißt es. Das werde die Entwicklung moderner Applikationsarchitekturen für das System i beschleunigen.

Erste Auswirkung der Umstrukturierung: Die Programmierwerkzeuge für das Editieren, Kompilieren und die Fehlersuche sind nunmehr in einem neuen Paket namens Rational Developer for System i (RDi) erhältlich.

Was ist anders an i5/OS?

Bis ans Ende der 70er-Jahre reichen die Wurzeln des heutigen System i zurück, denn es ist der Erbe der AS/400, die IBM wiederum am 21. Juni 1988 als Nachfolgemodell der beiden Baureihen System/38 und System/36 ankündigte. Alle Komponenten sind integriert, seien es Peripheriegeräte wie Drucker oder Speichersysteme, sei es die Middleware wie Datenbank und Transaktionsmonitor oder seien es Internet-Lösungen (Websphere), Dokumentenmanagementsysteme (Content Manager) oder Groupware (Lotus Domino). Dazu kommen die nötigen Werkzeuge für das Netz- und Systemmanagement sowie die Anwendungsentwicklung ebenso wie Software von IBM-Partnern wie SAP, Oracle, Lawson, Infor, SoftM, Oxaion oder GUS.

Anders als andere Betriebssysteme bildet i5/OS als reines Server-Betriebssystem nicht nur die Schnittstelle zu den Anwendungsprogrammen, sondern setzt selbst auf eine bereits in den 80er-Jahren definierte Schnittstelle auf: das Technology Independent Machine Interface (TIMI).

Es verfügte von Anfang an über eine 128-Bit-Architektur, die ihm 1995 einen fast unmerklichen Wechsel der Prozessorarchitektur von 48-Bit-CISC auf den 64-Bit-RISC-PowerPC gestattete. Das TIMI erleichtert aber nicht nur dem Betriebssystem derartige Technikwechsel, sondern federt sie auch für die Anwendungen so ab, dass zwanzig Jahre alte Programme heute noch unverändert ablauffähig sind.

i5/OS selbst fungiert als eine objektbasierte Datenbankmaschine – sprich die Datenbank ist in das Betriebssystem integriert. Das erspart nicht nur Kauf und Installation einer separaten Datenbank, sondern vereinfacht auch den Systembetrieb deutlich, da das Betriebssystem die Datenbank mitverwaltet. Nebenbei bemerkt können Datenänderungen automatisch transaktionsorientiert ablaufen, da ein Transaktionsmonitor ebenfalls in das Betriebssystem integriert ist. Textdateien gibt es übrigens nur als Emulation und aus Gründen der Kompatibilität mit anderen Betriebssystemen; in der Regel ist eine AS/400-Datei aber ein Datenbankobjekt.

Alles ist ein großer Speicher

Objektbasiert heißt in diesem Zusammenhang übrigens nicht „objektorientiert“ im Sinne des Software-Engineering. Es meint vielmehr, dass grundsätzlich jedes Element im System – ob Programm, Datei, Bibliothek, Benutzerprofil oder Gerätekonfiguration – ein Objekt mit bestimmten Funktionen und Eigenschaften ist. Die Eigenschaften lassen sich nur in begrenztem Umfang ändern. Beispielsweise kann man eine Textdatei nicht in das System transferieren und sie anschließend in ein Programm umwandeln, was die Vermehrung von Viren auf dem System i ausschließt.

Zudem arbeitet i5/OS nach dem Einspeicherkonzept (Single Level Storage). Das heißt: Die Anwendungen müssen nicht zwischen Haupt- und Plattenspeicher unterscheiden. Vielmehr stellt sich der gesamte Speicherplatz als linearer Raum dar, den das Betriebssystem verwaltet und die optimale Zuordnung der Objekte auf ein spezielles Plattenlaufwerk vornimmt. Für das Operating vereinfacht sich das Speichermanagement insofern, als es neue Ressourcen einfach an den linearen Speicher anhängt. Das Betriebssystem optimiert zugleich die Zugriffszeiten, indem es per Paging Daten von der Platte in den Hauptspeicher verlagert und umgekehrt.

Für die Benutzer besteht der augenfälligste Unterschied zu anderen Systemen darin, dass sie die gewohnte Programmfunktion „Speichern“ („Save“) gar nicht benötigen. Selbst wenn der Rechner abstürzt, bleiben die Daten nach dem Neustart verfügbar. Last but not least ist der Single Level Storage aus Sicht der objektorientierten Programmierung eine elegante Methode, automatisch für die nötige Persistenz von Objekten zu sorgen. Auf allen anderen Plattformen sind dazu beträchtliche Anstrengungen nötig.

Richtet sich diese Suite an die klassischen RPG-Programmierer, sind in dem ebenfalls neuen RDi SOA zusätzlich die für eine Entwicklung von Webapplikationen gedachten Tools wie der Rational Business Developer enthalten – früher als Enterprise Generation Language (EGL) bekannt. Zudem hat IBM in HATS for 5250 die bisher separaten Tools für Host Access Transformation Services und Webfacing in einem Produkt gebündelt.

Ebenfalls verbessern will IBM die Unterstützung von Open-Source-Lösungen wie Apache, Tomcat und PHP durch i5/OS. Kernstück ist die Integration der MySQL-Datenbank. Der MySQL Community Server für i5/OS steht auf mysql.com zum kostenlosen Download bereit – allerdings ohne jeden Support. Dagegen ist für den ab August 2008 verfügbaren MySQL Enterprise Server für i5/OS über mysql.com oder bei IBM eine jährliche Lizenzgebühr fällig – und zwar mit vier unterschiedlichen Support-Stufen. Die Enterprise Edition der drei großen System-i-Modelle 550, 570 und 595 hat IBM selbst um die PHP-Entwicklungsumgebung Zend Core für i5/OS (Standard Support) sowie MySQL Enterprise für i5/OS (Silber-Support) ergänzt. Zugleich positioniert IBM seine DB2 for i5/OS als MySQL Storage Engine.

Fazit

Nach den aktuellen IBM-Planungen gilt es als ausgemacht, dass V6R1 die letzte i5/OS-Release sein wird, die noch ältere Maschinen der 8xx-Modellreihen unterstützt. Zudem ist sie die erste Release, die nicht mehr auf den System i-Modellen 270, 820, 830 und 840 läuft. Darüber hinaus soll der Support für den Vor-Vorgänger V5R3 im April 2009 auslaufen. Den Vertrieb von V5R3 hat Big Blue bereits im Januar eingestellt. Upgrades auf die neue Version sind sowohl von V5R3 als auch von V5R4 direkt möglich.

Die Preise des Betriebssystems stehen für den deutschen Markt noch nicht fest. In USA bleiben sie IBM-Angaben zufolge unverändert. Danach kostet eine Lizenz pro Prozessor je nach dessen Leistung zwischen 1795 Dollar für das Einstiegssystem und 53 000 Dollar für die Topmodelle i570 und i595.

Betrachtet man die Entwicklungslinie des Betriebssystems, lässt sich als Zielrichtung ganz klar die Öffnung der einstmals höchst proprietären AS/400 ausmachen. IBM hat offenbar erkannt, dass heute jeder Mittelständler eine x86-Landschaft besitzt. Darin kann i5/OS als Klammer für das Management unterschiedlicher Windows-, Linux- und Unix-Server dienen.

Auch wenn sich die Hardware der Servermodelle immer weiter annähert und beispielsweise System i und System p heute praktisch baugleich sind, bleiben es doch grundverschiedene Systeme. Denn den Unterschied macht nicht die Hardware, sondern die Applikationen und Lösungsansätze. Gerade das neue i5/OS zeigt, in welche Richtung diese Differenzierung des System i voranschreitet. (sun)

BERTHOLD WESSELER

ist freier Journalist in Brühl.



Das Ende der Bild-Captchas

Gestaffelte Abwehr

Jörn Wagner

Captchas aus verzerrtem Text sind zwar ein beliebter Sicherheitsmechanismus. Jedoch bereitet ihre Lösung Anwendern häufig zu viel Mühe, und Computern fällt es leichter als erwünscht. Andere Verfahren stören weniger und sind ebenso zuverlässig.

Im Januar stellte *iX* eine Methode vor, mit PHP sogenannte Bild-Captchas zu erstellen [1]. Ein Captcha (Completely Automated Public Turing Test to Tell Computers and Humans Apart) soll Menschen von Softwarerobotern (Bots) unterscheiden. Dazu dienen häufig Bilder, aus denen der Anwender versteckte Buchstaben und Zahlen in ein Textfeld übertragen muss. Obwohl wesentlich bessere Captcha-Verfahren existieren, halten sich die Bildchen hartnäckig.

Es gibt verschiedene Gründe für die Anwendung von Captchas und damit verbundene Einsatzgebiete. Von Blogs, Foren und sozialen Netzen über freie Mail-Angebote bis hin zu Banken – viele Dienste setzen ein Captcha als Schutz vor dem automatisierten Missbrauch ein. Dabei geht es ebenso um die Abwehr von Spam wie um den Schutz von Informationen, zum Beispiel bei einer Seite mit Börsenkursen oder einer Onlineumfrage. Das simple Prinzip: Ein oder mehrere Tests entscheiden, ob die Eingabe von einem Menschen oder einem Programm stammt. Die Umsetzung dagegen ist knifflig und fehlerbehaftet.

Ein ideales Captcha erfüllt folgende Bedingungen:

1. Heutige Computer können den Test nicht lösen.
2. Menschen können ihn (meistens) lösen.
3. Es lassen sich neue Frage-Antwort-Kombinationen generieren.
4. Menschen sollen den Test in möglichst kurzer Zeit lösen.

Als Alan Turing 1950 den Test formulierte, glaubte er, dass Computer 50 Jahre später einem Anwender nach einem fünfminütigen Dialog in 70 % der Fälle vorgaukeln könnten, sie seien menschlich. Da sich diese vier Vorgaben beeinflussen, gibt es bisher kein Verfahren, das alle erfüllt und so perfekt Menschen von Maschinen unterscheidet.

Wer verzerrten Text entziffern kann

Als De-facto-Standard hat es sich durchgesetzt, verzerrte, schlecht zu erkennende Texte anzuzeigen und den Benutzer zu fragen, was er lesen kann. Die Bildchen mit wirren Mustern und schlecht erkennbaren Zahlen- und Buchstabenkombinationen erfüllen aber nur die dritte Bedingung. Denn Computer sind heutzutage in der Lage, mit Optical Character Recognition Texte aus einem Bild zu extrahieren. So arbeiten viele Projekte wie PWNtcha, Anti-Gimpy und aiCaptcha (siehe „Onlinequellen“) bereits erfolgreich an der Erkennung von Bild-Captchas, die unter anderem Yahoo, Microsoft, Paypal und die weit verbreitete Forensoftware phpBB einsetzen. Dass diese Seiten bisher noch nicht in großem Stil Ziel von Angriffen geworden sind, hängt nur damit zusammen, dass die Projekte ihren Code nicht veröffentlichen. Einzig von Anti-Gimpy gibt es eine öffentlich einsehbare Beschreibung des Algorithmus.

Die Zwickmühle bei der Verbesserung der Bild-Captchas ist schnell erklärt: Je aufwendiger es für den Computer ist, die Informationen zu erkennen, desto größer auch die Schwierigkeiten für Menschen. So sind Wörter im Allgemeinen besser zu erkennen als abstrakte Zeichenfolgen; allerdings basiert der Test dann auf einem begrenzten Wortschatz. Damit verletzt er die dritte Bedingung, da sich keine neuen Frage-Antwort-Kombinationen generieren lassen. Verzerrt man die Zeichen immer stärker und überlagert sie mit Störungen, fällt es sogar sehr gut sehenden Menschen schwer, die richtige Zeichenfolge zu erkennen.

Solche Falscherkennungen steigern vor allem die Frustration beim Anwender. Auf einer bekannten

deutschen Studentenseite ist für beinahe jede Aktion ein Captcha zu lösen, was die Zeit zur Erledigung des Gewünschten schnell auf ein Vielfaches ansteigen lässt. Ein entnervter Benutzer besucht unter Umständen die Seite nicht mehr, wenn kein Nutzen den erhöhten Aufwand rechtfertigt.

Zudem diskriminiert das Verfahren Menschen mit Sehschwächen, etwa Farbfehlsichtigkeiten, denen es unter Umständen schwerer fällt, den Test zu bestehen als einem Spam-Bot. Bild-Captchas sind also von Maschinen zu knacken, von Menschen dagegen immer seltener und lassen sich, wenn sie gut sind, nicht schnell lösen. Es gibt allerdings Alternativen.

Neben verzerrten Bildern findet man hin und wieder auch die einfache Aufforderung „Geben Sie folgenden Sicherheitscode ein“ und ein Feld namens „Sicherheitscode“. Sogar dieser geringe Schutz reicht oft aus. Obwohl ein wenig semantische Analyse für das Knacken erforderlich ist, kann man für jedes Verfahren einen eigenen, einfachen Angriff entwerfen. Damit besteht der einzige Schutz darin, dass nicht viele Seiten es einsetzen und sich der Aufwand für den Angreifer deshalb nicht lohnt.

Warum jede Lösung richtig ist

Ein weiteres Verfahren namens Anti-Captcha geht sogar noch einen Schritt weiter in Richtung Unsicherheit: Statt der Lösung soll man einen beliebigen anderen Text eingeben. Dies hilft vielleicht gegen Bots, die zufällig auf das verwendete Verfahren trainiert sind, weil sie fälschlicherweise den Code richtig eingeben. Allerdings öffnet es Tür und Tor für falsch programmierte, schlecht arbeitende und überhaupt nicht trainierte Bots. Denn statt einer gelten unendlich viele Lösungen. Die Hauptmotivation ist hier, die Hürde für den Benutzer niedrig zu halten.

Die Netbank sichert den Zugang zu Onlinekonten auch durch ein visuelles Captcha. Um Menschen mit Sehbehinderungen nicht auszuschließen, bietet sie ein auditives Captcha (oder Soundcha) an, das die Ziffern einzeln mit großen Pausen „vorliest“. Das eröffnet jedoch eine einfache Angriffsmöglichkeit, da der Vorrat an Tonschnipseln auf zehn begrenzt ist und sie sich durch die Pausen und die deutliche Aussprache gut voneinander unterscheiden lassen. Eine Verzerrung, wie früher bei Hotmail, würde wiederum die Barriere für Menschen mit schlechtem Hör- und Sehvermögen erhöhen. Zudem setzen Soundchas zu viel voraus: Der Benutzer darf sich nicht in einer lauten Umgebung befinden oder in einer, die das Abspielen von Geräuschen verbietet, er muss mit Sprache und Dialekt des Sprechers vertraut sein, eine funktionsfähige Soundkarte besitzen und sein Betriebssystem muss das verwendete Audioformat wiedergeben können.

Bereits Ende 2005 veröffentlichte das World Wide Web Consortium einen Artikel, der logische Puzzles, Nutzungsbeschränkungen und heuristische Tests vorschlug. Logische Puzzles sind zum Beispiel die (vermeintlich) leichten Fragen „Was ergibt 1 + 1?“ oder „Welches Tier macht ‚miau‘?“. Die erste ist jedoch ziemlich gut maschinenles- und

Onlinequellen

PWNtcha	sam.zoy.org/pwntcha/
Anti-Gimpy	www.cs.sfu.ca/~mori/research/gimpy/
aiCaptcha	www.brains-n-brawn.com/aiCaptcha
Anti-Captcha	www.timtucker.com/weblog/?p=74
Netbank	https://banking.netbank.de/wps/netbank-online-banking.jsp?blz=20090500
Formularfeld ausblenden	bueltge.de/spam-mit-hilfe-von-css-bekaempfen/473/
NoBot	www.asp.net/AJAX/AjaxControlToolkit/Samples/NoBot/NoBot.aspx
Plug-in für Wordpress	bueltge.de/wp-js-antispam-plugin/418/
Spam for Porn	www.boingboing.net/2004/01/27/solving-and-creating.html
Turing-Artikel	www.loebner.net/Prizef/TuringArticle.html
Breaking a visual Captcha	www.cs.sfu.ca/~mori/research/papers/mori_cvpr03.pdf

-lösbar, und bei der zweiten ergeben sich andere Zweifel: Was soll mit Eingaben wie „katse“ passieren? Ist „Kater“ ebenfalls richtig? Versteht der Benutzer die Frage noch, wenn sie auf Englisch gestellt wird? Sind dann Eingaben wie „cat“, „chat“ und „felino“ gültig? Außerdem bieten solche Puzzles immer nur einen begrenzten Fragenschatz und verletzen damit ebenfalls die Bedingung, dass sich neue Frage-Antwort-Kombinationen erzeugen lassen. Bei mathematischen Aufgaben ist dies nicht so, allerdings könnten Rechnungen der Art „Bilden Sie die Quadratwurzel aus der achten Potenz vom Zehner-Logarithmus von einhundert“ Benutzer vergraulen.

Wenn das Textfeld ausgefüllt ist

Heuristische Tests auf Schlüsselworte haben dieselben Nachteile wie aktuelle Anti-Spam-Software: Ihre Qualität hängt von den verwendeten Algorithmen und von der Pflege der Black- und Badword-Listen ab. Damit entbrennt ein stetiges Wettrennen zwischen Spammern und Captcha-Herstellern.

Ein Formularfeld per CSS auszublenden und bei ausgefülltem Feld den Zugriff zu verweigern, basiert auf dem Verhalten von Spam-Bots, mangels semantischer Analyse jedes Feld auszufüllen, um überall ihre Werbebotschaft zu hinterlassen. Alternativ könnte man den Wert von Standardfeldern wie „Name“ prüfen – im Blog des Autors finden sich viele Spam-Kommentare von „Name“ (die Standardbelegung).

Microsofts ASP.Net Control „NoBot“ hält sich im Grunde an die vom W3C vorgeschlagenen Nutzungsbeschränkungen und prüft, wie schnell der Benutzer das Formular absendet (Menschen brauchen länger als drei Sekunden) und wie häufig er dies tut (Spammer liefern meistens viele Nachrichten hintereinander ab). Zusätzlich führt es eine Rechnung in Javascript durch, deren Ergebnis stimmen muss. Streng genommen prüft es hierbei nicht, ob ein Mensch das Formular benutzt, sondern nur, ob ein Javascript-fähiger Browser verwendet wird. Allerdings erfüllt dieses Verfahren immerhin alle Bedingungen außer der zweiten. Bei abgeschaltetem Javascript weist dieses Verfahren einen Mensch immer ab.

Eine möglichst effiziente Kontrolle sollte mehrere Verfahren kombiniert anwenden. Zwar bietet eine transparente Lösung nicht notwendigerweise mehr Sicherheit als ein Bild-Captcha, belästigt aber immerhin den Benutzer nicht.

Für Wordpress existiert ein Plug-in, das ein logisches Puzzle benutzt, aber die Antwort bei aktiviertem Javascript automatisch gibt. Der Autor konnte damit den Spam in seinem Blog eliminieren, ohne dass die Benutzer etwas von dem Test merken.

Was das Kombinieren bringt

Kombiniert man dieses Vorgehen mit den oben genannten Nutzungsbeschränkungen und Verhaltensauffälligkeiten von Bots, hat man einen effektiven und für den Benutzer komfortablen Turing-Test. Eine zusätzliche Prüfung, ob das Gegenüber einen handelsüblichen Browser einsetzt, schadet nicht, da Spammer häufig selbstgeschriebene Programme verwenden. Sie sollte allerdings nicht den manipulierbaren User-Agent-String auswerten, sondern eher browserspezifische Variablen und Verhaltensweisen, die unter anderem bei Javascript-Weichen zum Zuge kommen.

Fast nebenbei beseitigt man so eine weitere Schwachstelle von Bild-Captchas: Selbst das beste, das ein Computer nicht erkennt, jeder Mensch aber identifizieren kann, ist anfällig für einen verteilten Angriff, auch bekannt als „Spam for Porn“. Dabei bekommt der Besucher einer anderen Webseite das zu lösende Captcha angeboten, das kostenlosen Zugriff auf für ihn interessante Informationen gewähren soll. Unwissentlich löst er die Aufgabe für den Spammer, der sich dadurch als Mensch ausgeben kann. Bei einem kombinierten Ansatz müsste der Übeltäter das gesamte Browserfenster präsentieren, damit sein Bot alle Tests besteht. Und das sollte auffallen.

Fazit

Webseiten werden oft von Bots heimgesucht. Zur Abwehr dienen sogenannte Captchas. Die häufig verwendeten Bild-Captchas haben jedoch zwei Schwachpunkte: Sie sind von Computern zu lösen und verursachen bei Menschen immer öfter Frustration und Zeitverlust.

Gerade wer das Verfahren für sicherheitskritische Anwendungen wie Onlinebanking einsetzt, sollte es überprüfen, um dem Benutzer keine falsche Sicherheit vorzugaukeln. Es gibt eine Reihe weiterer Tests, deren Kombination sicherer und komfortabler funktioniert als Bild-Captchas. (ck)

JÖRN WAGNER

ist Diplomand im Fach Wirtschaftsinformatik an der Universität zu Köln und arbeitet freiberuflich als Softwareentwickler.

Literatur

[1] Hubert Benjamin Ritzdorf; Webprogrammierung; Captchas in PHP; Mensch oder Maschine; *iX* 1/2008, S. 142

[2] Alan M. Turing: Computing Machinery and Intelligence, Mind, vol. LIX, no. 236, October 1950, pp. 433-460

[3] L. von Ahn, M. Blum, J. Langford: Telling humans and computers apart (automatically), CMU Tech Report CMUCS-02-117, February 2002

Steirischer Landtag: Komplett elektronisch

Digitales Parlament

Gabriele Ostanek

Gesetzgebung und Schriftverkehr im Landtag Steiermark erfolgen seit Oktober 2005 ausschließlich in elektronischer Form. Da das Projekt seither klaglos läuft, wollen andere Institutionen in den nächsten Jahren den gleichen Weg gehen.

Abgeordnete, die ihre Arbeit ausschließlich via Laptop erledigen, mögen für viele eine ferne Zukunftsvision sein. Im österreichischen Bundesland Steiermark ist das jedoch seit mehr als zwei Jahren Praxis. Denn als erstes Parlament mit Gesetzgebungskompetenz in Europa hat der Landtag Steiermark die gesamte Gesetzgebung auf papierlose Prozesse umgestellt. Alle parlamentarischen Abläufe einschließlich der Protokollierung der Sitzungen werden durchgängig elektronisch abgebildet. Damit ist das parlamentarische Prozedere unabhängig von Ort und Präsenz der Abgeordneten im Landtag (ausgenommen mündliche Verhandlungen).

Das Projekt mit dem einprägsamen Namen Pallast (Papierloser Landtag Steiermark) hat der Landtag im Herbst 2003 beschlossen. Seit Beginn der XV. Legislaturperiode im Oktober 2005 arbeitet das System erfolgreich. Bis heute ist das steirische Parlament das einzige, das ein digitales System „für alles“ betreibt. Zwar verwenden andere Parlamente ebenfalls Software für ihre Arbeit, jedoch deckt die immer nur Teilaspekte ab. In den nächsten Jahren wollen weitere Parlamente dem steirischen Beispiel folgen und umfangreiche papierlose Systeme einführen. Am weitesten fortgeschritten ist dabei der Landtag Brandenburg. Hier liegt mittlerweile ein Feinkonzept für ein ähnliches Workflowsystem vor.

Zielvorgabe in der Steiermark: die Verlagerung aller Prozesse und die Ablage der Daten in ein zentrales und sicheres Onlinesystem. Beispielsweise wollte man das Versenden von vertraulichen Dokumenten per E-Mail, Fax oder als Papierkopie vermeiden. Die bisherigen Kommunikationswege sollten durch ein einheitliches System laufen, auf das alle Beteiligten auf Basis eines Rollenkonzepts Zugriff haben.

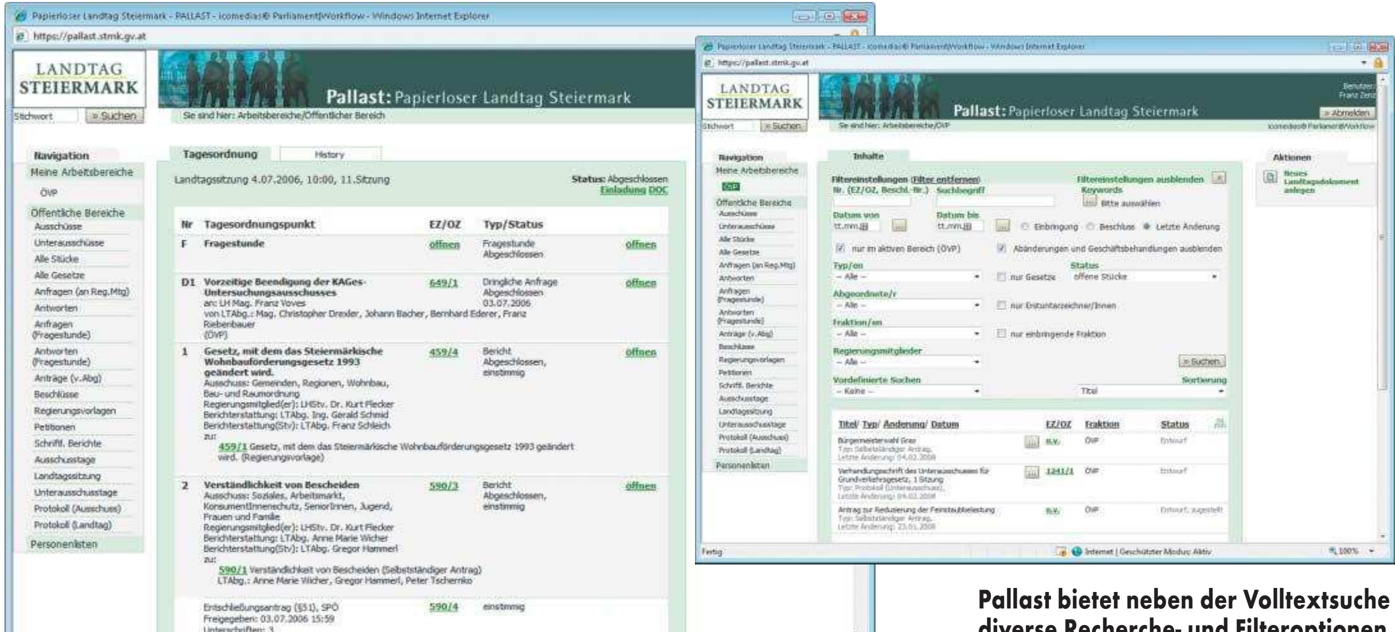
Ein weiterer Aspekt der Strategie war das Überprüfen und Verbessern der Geschäftsprozesse für die digitale Bearbeitung. Die Workflows sollten die bestehenden Papierabläufe jedoch nicht eins zu eins abbilden, sondern die Vorteile beider Welten – Papier und Elektronik – sinnvoll kombinieren.

Erfolg durch Beteiligung aller

Abgeordnete, Mitarbeiter der Landtagsdirektion, der Landesverwaltung, der Landesregierung sowie Experten der Firma Icomedias Systemhaus bildeten das Projektteam. Im Rückblick lässt sich das frühe Einbinden aller Interessengruppen als ein wesentliches Kriterium für den Erfolg des Vorhabens verbuchen. Gemeinsam legten die Beteiligten klare und verständliche Ziele fest. Jeder wusste, wohin die Reise geht und was ihn am Ende erwartet. Besondere Aufmerksamkeit genoss ein kontinuierliches Änderungsmanagement. Die Einführung von Pallast bedeutete schließlich nicht nur einen organisatorischen Wandel in der Verwaltung, sondern auch eine grundlegende Änderung der gewohnten individuellen Arbeitsweise und Arbeitsumgebung. Denn mit dem Stichtag der Inbetriebnahme mussten alle Abgeordneten und Mitglieder der Landtagsdirektion mit dem System arbeiten – ohne Ausnahmen und Alternativen.

In nur zwölf Monaten setzte das Projektteam Pallast um. Alle 56 Landtagsabgeordneten bekamen Laptops; jede Fraktion wie auch die Landtagsdirektion erhielten eigene geschützte elektronische Arbeitsbereiche. Alle Teilnehmer melden sich gesichert durch digitale Signatur und verschlüsselt durch SSL am System an. Die verfügbaren Dokumente und zu erledigenden Aufgaben ergeben sich aus dem individuellen Benutzerprofil: Fraktionszugehörigkeit, Stelle und Funktion. Insgesamt sind 36 vollständig modellierte und elektronisch umgesetzte Prozesse mit über 1000 Einzelstufen verfügbar.

Zentrales Element von Workflows und Dokumentenlenkung ist die Adressierung an einen oder mehrere Empfän-



Alle parlamentarischen Abläufe können die Abgeordneten lückenlos nachvollziehen (Abb. 1).

Pallast bietet neben der Volltextsuche diverse Recherche- und Filteroptionen (Abb. 2).

ger und Empfängergruppen – etwa Abgeordnete oder Ausschussmitglieder. Je nach Arbeitsablauf wählt der Benutzer verschiedene Reaktions-, Verständigungs- und Eskalationsmechanismen. Freigaben und Signaturen kann er sequenziell, parallel oder bis zum Erreichen einer Mindestunterschriftenzahl einstellen. Der Ersteller ordnet jedes Dokument seinem Typ entsprechend ein und den entsprechenden Workflows zu. Zusätzlich ist es möglich, für jedes Dokument thematische Zuordnungen zu wählen und Indizierungsbegriffe zu definieren (vorbereitend für die Parlamentsdokumentation).

Transparenz durch klaren Workflow

Die Empfänger bekommen die Dokumente, etwa Anträge, Tagesordnungen und Beschlüsse, in einem definierten Workflow zugestellt. Aus den Zustell- und Leseprotokollen lässt sich jederzeit ersehen, wann wer welche Inhalte zur Kenntnis genommen und wann er sie gelesen, freigegeben oder unterschrieben hat. Je nach Berechtigung können alle Beteiligten die detaillierten Änderungsprotokolle der Landtagsdokumente einsehen. Historische Versionen werden systematisch protokolliert. Eine sogenannte Lebenszyklusverfolgung garantiert die lückenlose Nachvollziehbarkeit aller Dokumente, Verhandlungen und Ergebnisse (Abbildung 1).

Alle neu anzulegenden Workflow-Dokumente bekommt der Ersteller als elektronische Vorlage. Sie sind nach Dokumententypen sortiert hinterlegt, zum Beispiel für einen Antrag an das Plenum oder eine neue Tagesordnung für eine Ausschusssitzung. Je nach Art des Schriftstücks belegt das System das Titelblatt mit einer Kopfstanze des Landtags. Die prozessspezifischen Darstellungsvorlagen verhindern Formfehler. In den so erzeugten und automatisch indizieren Dokumenten kann der Anwender sofort nach Freigabe im Volltext recherchieren. Um die Suche einzugrenzen, bietet sich die Definition von Filtern an, etwa nach Themen, nach Ersteller, nach verschiedenen Bereichen, nach Prozess oder nach Fristen (Abbildung 2).

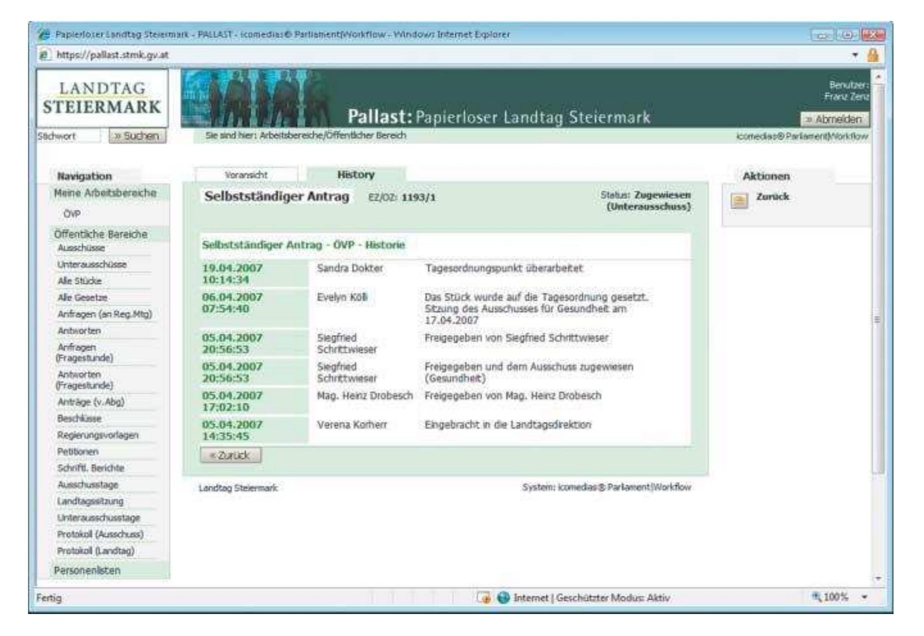
Pallasts Sicherheitsarchitektur garantiert den Schutz aller vertraulichen Informationen. Der Zugang zu den Daten ist mehrfach gesichert, die Datenübertragung ausnahmslos verschlüsselt. Erstmalig hat man dazu die österreichische Bürgerkarte in einen USB-Stick integriert. Die von Icomedias Systemhaus entwickelte Lösung hat der Akkreditierungsdienstleister A-Trust (www.a-trust.de) als SIM-Karte eigens für den Landtag Steiermark hergestellt. Abgeordnete und Mitarbeiter von Fraktionen sowie der Landtagsverwaltung können das webbasierte System von überall her benutzen.

Die in der Anwendung gespeicherten Daten unterliegen strengen Schutzvorschriften. Insbesondere gilt das für die Authentizität etwa von Gesetzesvorlagen. Aus diesem Grund ist der Einsatz der qualifizierten elektronischen Signatur im gesamten System obligatorisch. Die Anmeldung erfolgt ebenfalls mittels Signatur, sodass nur berechtigte Benutzer die Dokumente ändern können. Jede Kommunikation zwischen Server und Client läuft verschlüsselt.

Entscheidend für die Akzeptanz eines solchen Systems ist eine hohe Ausfallsicherheit. Aus diesem Grund läuft Pallast auf einem hochverfügbaren Linux-Cluster mit redundantem Cluster-Manager im Sicherheitsrechenzentrum der Steiermärkischen Landesregierung. Seit Oktober 2005 arbeitet das System

iX-TRACT

- Der Steirische Landtag ist das einzige Parlament in Europa, das Gesetzgebung und Schriftverkehr komplett digital abwickelt.
- Hauptkriterien für die gute Akzeptanz des Systems sind seine einfache Bedienbarkeit, seine Zuverlässigkeit sowie die Einbindung aller relevanten Gruppen in Konzeption und Umsetzung.
- Da die Onlineanwendung seit über zwei Jahren anstandslos läuft, wollen andere Institutionen und Landesparlamente ähnliche Projekte starten.



Da jeder Berechtigte alles Wichtige sofort sieht, spart sich der Landtag beispielsweise Massenkopien (Abb. 3).

ununterbrochen nach dem Verfügbarkeitslevel AEC-2 (Availability Environment Classification, High Availability). Laut Messung beliefen sich die Ausfallzeiten der zentralen Cluster jährlich auf weniger als 15 Minuten. Das Gesamtsystem basiert weitgehend auf Open-Source-Software, Programmiersprachen sind Java und PHP, die Datenbank heißt PostgreSQL 8.0.

Dokumente, im Landtag Steiermark auch „Stücke“ genannt, legt Pallast als strukturierten Inhalt in XML ab. Die Bearbeitung ist mithin nicht an ein Format wie *.doc* gebunden. Ein herkömmliches Dokumentenmanagement- oder Vorgangsbearbeitungssystem (DMS/VBS) ist hier nicht involviert, denn es hätte den Nachteil, dass es Dokumentdateien speichert. Pallast übernimmt die Aufgaben eines VBS/DMS-Systems, was den Workflow und die Versionierung betrifft. Die Inhalte gibt es nach Bedarf in verschiedenen Formaten (*.doc*, *.odt*, PDF) sowie für verschiedene Medien aus. Dies erfolgt im Wesentlichen über XSL-Transformationen, die auf eine aus der Datenbank erzeugte XML-Struktur angewendet werden. Darüber gewinnt man eine Flexibilität, die es erlaubt, mobile Geräte wie PDAs oder Smartphones in den Workflow einzubinden.

Eine Kernforderung des Konzeptes war die einfache Bedienung der Onlineanwendung. Darauf legten die Entwickler in allen Projektphasen besonderes Augenmerk. Auch Personen mit wenig IT-Erfahrung können bereits nach einer halbtägigen Einarbeitung damit kompetent umgehen. Nutzungsstatistiken, die Zahl der im System überarbeiteten Dokumente sowie die Rückmeldungen an die Projektleitung zeigen, dass die Nutzer das System akzeptieren. Ein weiteres Indiz für die Zufriedenheit ist der Wunsch, es künftig auf die Landesregierung Steiermark, den Landesrechnungshof sowie den Bundesrechnungshof auszuweiten.

Wenn alle Tagesordnungspunkte für eine Sitzung freigegeben sind, stellt Pallast die relevanten Inhalte automatisch und umgehend auf der Website des Landtags Steiermark zur Verfügung. Alle bisher erforderlichen Maßnahmen und Aufbereitungen für die Publikation entfallen, da die Anwendung alle Dokumente wie beschrieben Template-basiert via XML erstellt. Das schafft ein bisher nicht gekanntes Maß an Transparenz von politischen Entscheidungen. Nicht nur die Medien, auch die Bürger nutzen das Portal in zunehmendem Maße.

Pallast ändert die Beschäftigungsstruktur des Landtags: Die ehemaligen Boten beschäftigen sich nun nicht mehr mit dem Verteilen von Papier, sondern scannen externe Eingänge, archivieren die elektronischen Dokumente und verteilen sie an die richtigen Adressaten. Da das Parlament als Zertifizierungsstelle österreichische Bürgerkarten ausstellen darf, kam es hier ebenfalls zu Höherqualifizierungen mehrerer Mitarbeiter, die nun die Sicherheit und Verwaltung von Zertifikaten gewährleisten sowie Signaturkarten erstellen.

Das System spart Zeit, Papier, Geld und CO_2 ein. Die elektronischen Arbeitsprozesse beschleunigen Verwaltungsabläufe um vier bis sechs Wochen. Beispielsweise konnte der Landtag durch das abgestimmte Zusammenspiel von Legistik (Rechtsförmlichkeit) und Technik auf die erste Lesung zur Ausschusszuweisung verzichten. Änderungs- und Entschließungsanträge können die Abgeordneten während einer Sitzung elektronisch unterschreiben und einbringen. Alle berechtigten Benutzer sehen sofort auf ihren Monitoren, was beantragt wird (Abbildung 3). Das ließ sich zuvor nur durch Massenkopien und umfangreiche Botengänge erledigen. Hinzu kommt: Abgeordnete müssen nicht persönlich im Landtag anwesend sein, um Anträge zu unterschreiben. Alleine durch die Kostensenkung bei der Landtagsdirektion, die sich etwa durch den Wegfall von Kopien und Versand ergibt, spart das Parlament jährlich rund 200 000 Euro. Die Abgeordneten verbrauchen 95 % weniger Papier.

Seit zwei Jahren arbeitet Pallast zur Zufriedenheit aller und wird dabei ständig weiterentwickelt. Einige Module haben die Entwickler im letzten Jahr neu erstellt, zum Beispiel für den Einsatz im Rahmen der fraktionsinternen Sitzungsvorbereitung und Auswertung. Weiterhin integrierten sie verschiedene Ansichten von Tagesordnungen und Dokumenten, persönliche Notizen der Abgeordneten sowie einen Freigabe-Workflow. Die Reorganisation des Stenografendienstes sowie der Live-Protokollierung während der Landtagssitzung befinden sich in der Umsetzungsphase.

Das System funktioniert klaglos

Alle Prozesse von den ersten vorparlamentarischen Entwürfen von Dokumenten, Fraktionsberatungen, Sitzungsmappen, Ausschussbehandlungen, Abstimmungen, elektronisch signierten Gesetzen bis hin zur zentralen Ablage, Archivierung und Verteilung von Dokumenten und Publikationen im Internet wickelt Pallast umfassend ab. In einer für derartige Projekte bemerkenswert kurzen Zeitspanne haben die Benutzer das System angenommen. Der Landtag Steiermark ist das europaweit erste durchgehend digitale Parlament und wurde mehrfach ausgezeichnet. Unter anderem erhielt das Projekt einen Jurypreis beim Österreichischen Staatspreis Multimedia 2006 und das „Österreichische E-Government Gütesiegel“ des Bundeskanzleramts für sicheres und vertrauenswürdiges E-Government. (jd)

GABRIELE OSTANEK

arbeitet im Amt der Steiermärkischen Landesregierung, Abteilung Informationstechnik.

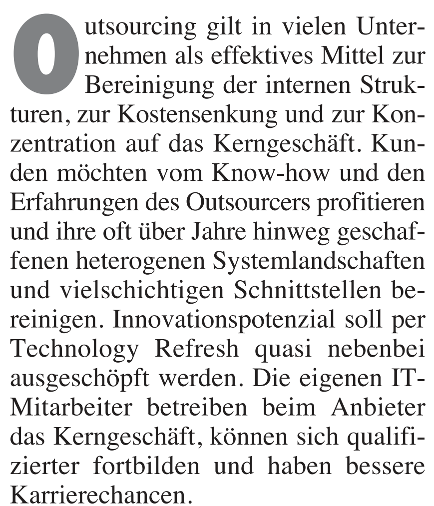
Zurückholen ausgelagerter Dienstleistungen

Alles auf Anfang

Georg Meyer-Spasche



Next-Generation-Outsourcing, Backsourcing, Insourcing – was kommt nach dem Outsourcing? Immer wieder liest man von gescheiterten Outsourcings und den Schwierigkeiten, sich voneinander zu trennen. Viele dieser Probleme lassen sich lösen.



Outsourcing gilt in vielen Unternehmen als effektives Mittel zur Bereinigung der internen Strukturen, zur Kostensenkung und zur Konzentration auf das Kerngeschäft. Kunden möchten vom Know-how und den Erfahrungen des Outsourcers profitieren und ihre oft über Jahre hinweg geschaffenen heterogenen Systemlandschaften und vielschichtigen Schnittstellen bereinigen. Innovationspotenzial soll per Technology Refresh quasi nebenbei ausgeschöpft werden. Die eigenen IT-Mitarbeiter betreiben beim Anbieter das Kerngeschäft, können sich qualifizierter fortbilden und haben bessere Karrierechancen.

Vor allem soll das Outsourcing in der Regel die Kosten senken, indem günstigere Einkaufsbedingungen des Anbieters genutzt, Systeme zusammengelegt und Mitarbeiter transferiert werden. Schließlich sind positive Cashflow-Effekte durch den Verkauf der IT-Landschaft an den Outsourcer zu realisieren. Dieses Potenzial vor Augen, versucht das Management oft, ein Outsourcing möglichst schnell zu realisieren – entsprechend groß ist der Zeitdruck in der Vorbereitung.

Inzwischen ist vielerorts Ernüchterung eingekehrt. Man hört und liest von kriselnden Projekten, ungeplanten Mehrkosten, mangelnder Flexibilität der Anbieter, Kontrollverlust der Kunden und Frustration für beide Seiten durch unklare Leistungsbeschreibungen und praxisferne SLA. Statistiken zufolge sind nur rund 30 % der Kunden zufrieden mit ihrem Outsourcing. Obwohl demnach 70 % unzufrieden sind, werden nur ganz wenige Outsourcings wirklich beendet – selbst wenn die Beteiligten den Vertrag regulär kündigen könnten.

Stattdessen wird der Vertrag oft zähneknirschend verlängert und damit eine wichtige Gelegenheit verpasst, vorhandene Probleme abzustellen. Das hat auch einen Grund: Es gibt diverse Stolperfallen und der Kunde geht bei einem Anbieterwechsel oder einem sogenannten Backsourcing erhebliche Risiken ein, die denen bei Vertragsbeginn ähneln oder sie sogar übertreffen.

Wer weiß noch, wie es geht?

Das fängt schon bei den Mitarbeitern an: Bei einem Backsourcing ist der Kunde besonders auf die Rückkehr seiner ehemaligen IT-Mitarbeiter angewiesen, denn er selbst hat ja kaum noch IT-Fachkräfte und müsste andere erst anlernen. Doch auch ein neuer Anbieter benötigt in aller Regel die erfahrenen Mitarbeiter aus dem endenden Outsourcing. Zwar enthält jeder Outsourcing-Vertrag Bestimmungen, nach denen alle dem outgesourcten Betriebsteil IT zugehörigen Mitarbeiter immer diesem Bereich folgen, erst zum Outsourcer, nach Vertragende wieder zum Kunden oder zum neuen Anbieter.

Leider ist jedoch die Zuordnung eines Mitarbeiters zu einem Betriebsteil nicht statisch: Der Anbieter setzt ihn recht schnell auch für andere Kunden ein. Damit wird diese Zuordnung zum outgesourcten Betriebsteil zunehmend unklarer – mit der Folge, dass die Rückkehr der ehemaligen Mitarbeiter alles andere als sicher ist. Die Rückkehrerquote sinkt weiter, wenn die Karrierechancen beim Anbieter spannender erscheinen. Das Problem wächst, je länger ein Outsourcing andauert und je weniger IT-Fachpersonal und Know-how noch im Kundenunternehmen vorhanden sind.

Die perfekte Lösung gibt es nicht und einer gewissen Fluktuation wird man immer ausgesetzt sein. Jedoch lassen sich die Auswirkungen begrenzen: Schon während des Outsourcings sollte man Maßnahmen ergreifen, die einerseits die Fluktuation bei wichtigen Positionen minimieren und andererseits sicherstellen, dass Know-how zum Beispiel im Betriebshandbuch dokumentiert wird und nicht einfach abfließt. Wenn man zusätzlich auf Standards statt proprietäre Abläufe setzt, lässt sich fehlendes Know-how leichter wieder aufbauen.

Sofern der Kunde Hardware an den Anbieter übertragen hat, ist das Thema in vielen Outsourcing-Verträgen scheinbar detailliert geregelt. Es gibt lange Assetlisten mit Aussagen über Eigentums- und Besitzverhältnisse, Miet- und Leasingverträge. Diese Listen erstellen die Beteiligten beim ursprünglichen Outsourcing, pflegen sie aber selten weiter. Bei einem Backsourcing oder einem Anbieterwechsel sind veraltete Listen unbrauchbar, denn schon nach wenigen Jahren ist der Großteil der Hardware ersetzt – Liste und Realität haben dann nichts mehr gemeinsam.

Solange die Hardware nur 1:1 im Rahmen des Technology Refresh ausgetauscht wird, lassen sich die Listen immerhin nachführen. Wenn sich im abzuwickelnden Outsourcing-Vertrag außerdem eine klare Regelung zur Kaufpreisbildung findet, Leasingverträge leicht übertragbar gestaltet sind und die Entsorgung alter Geräte festgelegt ist, sind die Hardwareklippen umschifft.

Wenn der Anbieter aber seinem Auftrag gerecht wird, Skaleneffekte und Synergien zu heben, sieht alles

anders aus: Werden Systeme etwa durch Virtualisierung konsolidiert, kann man die eingesetzte Hardware keinem Kunden klar zuordnen, da sie für viele Kunden eingesetzt wird. Hardwarelisten lassen sich in diesem Moment nicht mehr einfach aktualisieren. Kunden stehen dann schnell vor dem Dilemma, ihre Hardwarelandschaft neu planen und beschaffen zu müssen – was zumindest wertvolle Zeit kostet.

Die Erkenntnis, dass Konsolidierung und Innovation eine spätere Trennung erschweren, hat tatsächlich bereits dazu geführt, dass in einigen Outsourcing-Verträgen der Kunde seinem Anbieter ausdrücklich verbietet, Synergiepotenziale zu nutzen. Das mag den Ausstieg zwar erleichtern, der Kunde legt so aber einen Grundstein für den Misserfolg.

Andere übertragen die Assets gar nicht erst, sondern beauftragen ihren Anbieter mit dem Asset-Management. Den unbestrittenen Vorteil, Assets später nicht zurückübertragen zu müssen, erkauft man sich dabei jedoch einerseits mit deutlichen Mehrkosten durch den erhöhten Verwaltungsaufwand für Managed Services, andererseits sind auch hier den Synergien Grenzen gesetzt. Nachteilig kann sich diese Struktur zudem auf die Durchsetzbarkeit von Service Level Agreements (SLAs) auswirken, denn die Wartungsverträge bleiben beim Kunden und die Verantwortung ist im Falle eines Problems schwieriger nachvollziehbar.

Dabei ist es durchaus möglich, Hardwarelandschaften strukturell zu ändern, Synergien zu heben und dennoch ein Outsourcing sauber und schnell zu beenden oder auf einen neuen Anbieter zu übertragen. Je nachdem, inwieweit der Kunde proprietäre Systeme benötigt, kann der Weg etwa über eine weitere Standardisierung der Leistungen oder über ein Joint-Venture-Modell gehen. Die Standardisierung führt zum Beispiel im Rechenzentrum dazu, dass der Kunde keine Systeme, sondern nur noch MIPS, RAM und TByte in bestimmter Menge und Qualität vom Anbieter kauft. Ein Wechsel zu einem anderen Anbieter ist so leichter möglich und Preise sind besser vergleichbar.

Wird hingegen spezielle Hardware benötigt, kann sich ein Joint-Venture-Modell lohnen. Hier gründen der Kunde und der Anbieter ein gemeinsames Unternehmen, das die Assets hält und die Leistungen erbringt. Bei einem Backsourcing übernimmt der Kunde dann das Unternehmen zu 100 % und erhält die sich im Unternehmen befindlichen Assets und Ressourcen. Für ein Next-Generation-Outsourcing übernimmt die Geschäftsanteile der neue Anbieter. Dieses Modell kann viel leisten, eignet sich aber nicht für jeden Fall und ist mit Bedacht zu strukturieren, um nicht wieder Synergiepotenzial zu zerstören.

Vergleichsweise einfach ist die Rückübertragung von Individualsoftware des Kunden. Im Vertrag sind oft schon die richtigen automatischen Mechanismen vorgesehen, sodass man nur auf die vollständige Rückgabe achten muss.

Anders sieht es bei Software aus, die von Drittherstellern geliefert wird. Hier muss der Kunde häufig an den Dritthersteller für die Rückübertragung zahlen. Das ist meistens der Fall, wenn der Outsourcer bei Abschluss des Vertrages mit dem Dritthersteller nicht vereinbart hat, dass die Lizenz nach dem Outsourcing kostenfrei übertragen werden kann. Wenn der abzuwickelnde Outsourcing-Vertrag keine entsprechende Verpflichtung enthält oder der Anbieter nicht selbst darauf geachtet hat, entstehen so vermeidbare Kosten. Wartungs- und Leasingverträge lassen sich nach den gleichen Grundsätzen mobil halten.

Für die beim alten Anbieter gespeicherten Kundendaten gilt es zu klären, wie und an wen die Daten zu übergeben und dann beim alten Anbieter zu löschen sind. Sofern sich die Formate durch das Backsourcing beziehungsweise die Übergabe an den neuen Outsourcer nicht ändern, geht das in der Regel problemlos. Anders beim Wechsel in neue Systeme, hier ist entweder eine Datenmigration zu planen oder es müssen, etwa bei Datensicherungen, mithilfe des alten Anbieters Tools für den Lesezugriff gesichert werden.

Rückabwicklung nur Hand in Hand

Auch wenn manche Kunden es kaum wahrhaben wollen: Ohne Kooperation und Unterstützung des bisherigen Outsourcers auch nach dem eigentlichen Vertragsende funktioniert ein Backsourcing so gut wie gar nicht und ein Next-Generation-Outsourcing wird zumindest in der Übergangsphase stark behindert. Neben den schon beschriebenen Unterstützungsleistungen zur Übertragung von Know-how, Assets, Daten und Verträgen ist es oft erforderlich, dass der alte Anbieter für einen Übergangszeitraum noch Ressourcen vorhält, um den Betrieb auch bei Verzögerungen in der Übergangsphase zu sichern. Besonders notwendig ist die Zusammenarbeit nach einem Anbieterwechsel, denn im Rahmen der vorvertraglichen Sorgfaltsprüfung (Due Diligence) erhält der neue Anbieter naturgemäß oft nur unvollständige Informationen vom alten Anbieter, weil dem alten Anbieter oft gar nichts an dem Wechsel liegt. Nach dem Wechsel klappt der Informationsfluss meist besser.

Positiv auf die Migration wirkt sich häufig aus, dass es bei einer Trennung immer auch um die Reputation des alten Anbieters geht. In dieser Situation unternimmt er schon im eigenen Interesse vieles, um kooperativ zu erscheinen und keine möglichen Kunden abzuschrecken. Verlassen kann man sich darauf natürlich nicht.

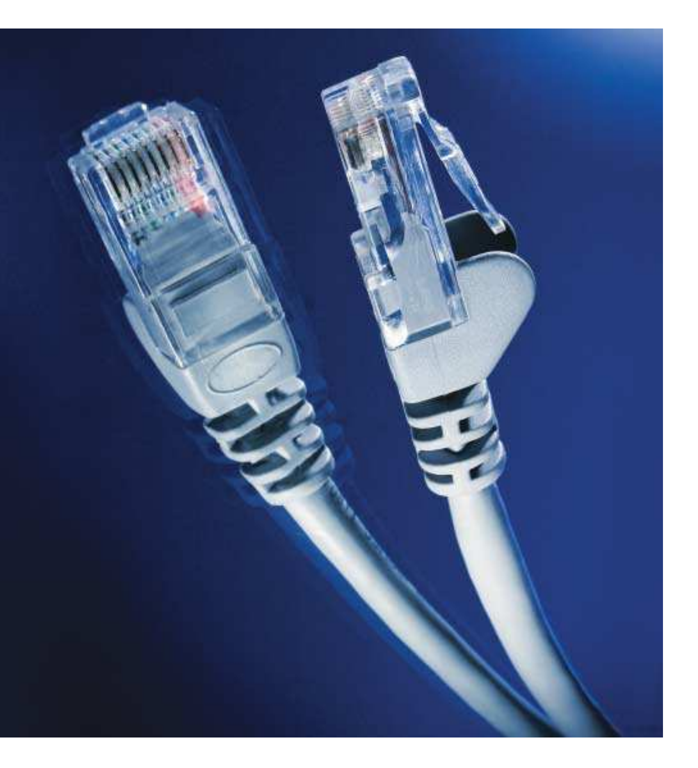
Das Beenden eines Outsourcings belastet den Kunden in der Regel stärker als den Anbieter: Letztlich muss der Kunde seinen Produktivbetrieb auch zukünftig sicherstellen. Er trägt die mit der Rück- oder Weiterübertragung der Betriebsmittel, der Mitarbeiter und des Know-hows verbundenen fachlichen und finanziellen Risiken.

Viele halten diese Risiken für unkalkulierbar und sehen deshalb von der Rückabwicklung oder Neuvergabe kriselnder Outsourcings ab. Das ist jedoch langfristig der falsche Weg, denn Abhängigkeit und Risiken werden dadurch nicht geringer. Außerdem vergibt man die Chance, die Qualität zu verbessern oder einfach vergleichbare Leistungen wieder strategischer am Markt nachzufragen – wie es das Outsourcing ja ursprünglich ermöglichen sollte.

Der richtige Weg ist, den Fall des Backsourcings oder Anbieterwechsels möglichst frühzeitig vorzubereiten, denn so werden die Risiken eher transparent und damit nicht nur kalkulierbar, sondern planbar. Im Idealfall beginnt man diese Planung parallel zu der des ersten Outsourcings, gestaltet die Verträge entsprechend und pflegt sie zusammen mit der Betriebsdokumentation. Aber selbst wenn der günstigste Zeitpunkt verpasst ist, lässt sich etwa durch ein gemeinsam mit dem Anbieter erstelltes Entflechtungskonzept noch viel retten. Wichtig ist nur, dass man sich nicht von einem gut laufenden Outsourcing abhalten lässt: Gerade in dieser Situation lassen sich tragfähige Entflechtungskonzepte gemeinsam viel einfacher aufsetzen als in der Krise oder unter Zeitdruck. (ur)

GEORG MEYER-SPASCHE

ist Rechtsanwalt für IT-Recht bei der Kanzlei Osborne Clarke in Köln. 



Das verteilte Dateisystem pNFS

Parallelwelten

Oliver Tennert

Datenintensive Applikationen für High Performance Computing müssen immer mehr Informationen in immer kürzerer Zeit bewegen. Neue Dateisysteme und Protokolle sollen dem Bedarf an skalierbaren Speicherkapazitäten und -bandbreiten Rechnung tragen sowie direkten, parallelen Zugriff mehrerer Clients ermöglichen. Eine Erweiterung des kommenden NFS 4.1 – Parallel NFS (pNFS) – soll das ebenfalls leisten.

Im High Performance Computing sind Datenaufkommen im Terabyte-Bereich keine Seltenheit. Schwierigkeiten bereitet weniger die Ablage der ruhenden Daten als die Performance des notwendigen Hin- und Herkopierens während der Berechnung, sei es von der Platte in den Hauptspeicher oder – im Falle von HPC-Clustern – von einem Knoten zum anderen. Außerdem hängt davon die Turnaround-Zeit eines Jobs ab.

Oft muss man diese Daten auf einen gemeinsamen Speicherbereich zwischenlagern. Typischerweise löst man die Aufgabe in HPC-Clustern, indem ein zentraler Dateiserver den Rechenknoten diesen Bereich per NFS zur Verfügung stellt. Das offenbart vor allem bei größeren Clustern auch gleich die Grundproblematik dieses Ansatzes: Der NFS-Server stellt einen Flaschenhals dar und kann den gebündelten Anforderungen aller Rechenknoten nicht mehr nachkommen. Die Lösung ist nicht neu: sogenannte parallele oder verteilte Dateisysteme. Sie tragen dem Bedarf an skalierbaren Speicherkapazitäten und -bandbreiten Rechnung und erlauben den direkten, parallelen Zugriff mehrerer Clients.

Ein Blick in die Geschichte

Verteilte Dateisysteme sind an sich nichts Neues: neben Klassikern wie dem Andrew File System (AFS) und dem daraus abgeleiteten, aber mittlerweile völlig veralteten DCE/DFS (Distributed Computing Environment/File System) existieren inzwischen mächtige und leistungsfähigere kommerzielle Produkte wie IBMs General Parallel File System (GPFS) oder SGIs Clustered XFS (CXFS). Die Open-Source-Lösung Lustre ist in der Linux-HPC-Welt ebenfalls schon recht weit verbreitet. Sie schickt sich nun nach dem Kauf der bei der Entwicklung federführenden Firma Cluster File Systems (CFS) durch Sun im Jahr 2007 an, auch in der Solaris-Welt Fuß zu fassen.

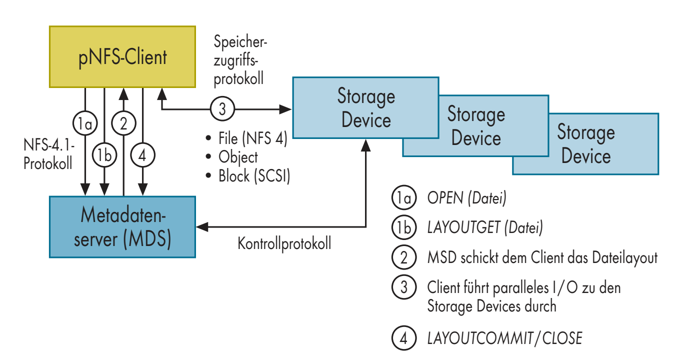
Neu ist, dass die IETF das altehrwürdige NFS in einer parallelen Version ebenfalls zum Internet-Standard erheben will – mit dem Ziel, Interoperabilität zwischen allen Betriebssystemen zu bieten. Das ursprüngliche Konzept für parallele NFS-Zugriffe beschrieb 2004 Garth Gibson, Professor an der Carnegie Mellon University (CMU) und späterer Gründer und CTO der Firma Panasas (siehe Onlinequellen [a]). Bekannt war Gibson bereits als Koautor des historischen „RAID-Papers“ von 1988 [1]. Diese Ursprünge sind im Design von pNFS deutlich erkennbar. Das von Panasas entwickelte hochperformante HPC-Dateisystem Activescale PanFS mit den weiter unten beschriebenen Object-Based Storage Devices als zentralen Komponenten ist im Wesentlichen die kommerzielle Fortführung des ebenfalls von Garth Gibson ursprünglich an der CMU begründeten Projekts „Network-Attached Secure Disk (NASD)“ [b].

Mittlerweile existiert Version 21 des Internet Draft zu NFS Version 4.1, deren bedeutendste Neuheit zweifellos Parallel NFS (pNFS) darstellt [c]. Namhafte Firmen wie EMC, IBM, Netapp und Sun schlossen sich dem Standardisierungsgremium an – niemand wollte es natürlich verpassen, rechtzeitig auf den Zug aufzuspringen.

Erklärtermaßen soll pNFS als Teil von NFS 4.1 nicht nur dessen Semantik in Bezug auf Cache-Konsistenz oder Sicherheit übernehmen, sondern auch eine möglichst einfache und in sich flexible Erweiterung des NFS-4-Protokolls darstellen. pNFS ist optional, NFS-4.1-Implementierungen müssen es also nicht beinhalten.

Architektur mit vielen Protokollen

Das pNFS-Protokoll führt eine Trennung von Meta- und Nutzdaten durch: Ein pNFS-Cluster besteht zum einen aus sogenannten Storage Devices, die die Nutzdaten des verteilten Dateisystems beherbergen, und einem Metadatenserver (MDS) – dem eigentlichen NFS-4.1-Server – der Informationen darüber bereithält, auf welchen Storage Devices und an welcher Position auf diesen sich Teile einer bestimmten Datei befinden, das sogenannte Layout. Die Referenzierung von Storage Devices erfolgt über sogenannte Device-IDs. Eine Liste aller Client-IDs und deren Zuordnung zu tatsächlichen Hostnamen bezie-



Die pNFS-Protokollarchitektur am Beispiel des schematischen Ablaufs der Kommunikation zwischen pNFS-Client und MDS sowie den Storage Devices beim Dateizugriff (Abb. 1)

hungsweise SCSI-LUNs oder Volume Names kann ein pNFS-Client über die RPC-Operation *GETDEVICELIST* erhalten. Neben diesen „Striping-Parametern“ speichert der MDS auch sämtliche anderen Metadaten wie Zugriffsrechte oder Ähnliches, die sich üblicherweise im Inode einer Datei befinden.

Clients und MDS kommunizieren untereinander über das neue NFS-4.1-Protokoll, und der NFS-Mount eines pNFS-Dateisystems erfolgt über den MDS. Das neue, dateisystemspezifische Attribut *fs_layout_type* gibt an, welche sogenannten Layout-Typen dieses Dateisystem unterstützt. Sie bestimmen das Speicherzugriffsprotokoll („Storage Access Protocol“), mit dem die Clients auf die Storage Devices zugreifen können. Bislang definiert NFS 4.1 drei potenzielle Speicherzugriffsprotokolle: datei-, block- und objektbasiert.

Will ein pNFS-Client auf eine bestimmte Datei oder Teile davon zugreifen, schickt er eine *OPEN*- gefolgt von einer *LAYOUTGET*-Operation an den MDS, der ihm das Layout für die Datei oder den entsprechenden Teil zurückliefert. Der Besitz des Layouts einer Datei stellt für den Client implizit auch das Recht dar, auf diese zuzugreifen.

Zu guter Letzt existiert ein Kontrollprotokoll („Control Protocol“), das MDS und Storage Devices zur Synchronisierung von Zustandsdaten verwenden. Dies ist im Standard absichtlich unspezifiziert, um Herstellern eine gewisse Flexibilität zu erlauben. Der NFS-4.1-Standard gibt aber Rahmenbedingungen für ein Kontrollprotokoll, beispielsweise zur Behandlung der Change-/Modify-Time-Attribute von Dateien.

Abbildung 1 zeigt schematisch die Abläufe beim Datenzugriff via pNFS. Diese

iX-TRACT

- Eine der großen Herausforderungen im High Performance Computing ist die Geschwindigkeit des Datentransports entweder vom Storage in den Hauptspeicher oder zwischen den Knoten eines Clusters.
- Bei Clustern wird ein NFS-Server zur Bereitstellung des gemeinsamen Speichers schnell zum Flaschenhals für die Turnaround-Zeiten eines Jobs.
- Mit dem kurz vor der Verabschiedung stehenden NFS 4.1 hält als Option pNFS Einzug in den NFS-Standard, das mit Parallelisierung des Datenzugriffs deutlich besseren Durchsatz verspricht.

Exemplarische pNFS-Client-Implementierung, wie sie im Großen und Ganzen bei Linux auch realisiert ist (Abb. 2).

Möglicher Aufbau eines pNFS-Clusters mit Load Balancing bei den MDS. Das Clustering der MDS selbst spezifizieren die Standards nicht (Abb. 3).

Art des asymmetrischen Zugriffs ist von Activescale oder Lustre wohlbekannt und stellt quasi eine Out-of-Band-Virtualisierung des globalen pNFS-Namespace dar. Sie entlastet den Metadatenserver vom eigentlichen Datenfluss und bietet eine Möglichkeit des parallelen Zugriffs auf Storage Devices über ein Transportnetzwerk.

pNFS sieht die Abwärtskompatibilität mit nicht-pNFS-fähigen NFS-4-Clients derart vor, dass in diesem Falle der MDS den Datenzugriff auf die Storage Devices im Namen des Clients vornimmt und diesen via NFS 4 die Daten bereitstellt. Der MDS fungiert dabei quasi als Proxy-Server.

Eine Frage der Layout-Typen

Ein pNFS-Client behandelt das vom MDS erhaltene Layout fast vollkommen opak: Er interpretiert nur die Information über das zu verwendende Speicherzugriffsprotokoll. Dieses bestimmt, welchen clientseitigen Layout-Treiber er zum Generieren eines IO-Requests einsetzt. Alle weiteren Informationen wie Striping-Parameter oder Capabilities reicht der Client unverändert an die Storage Devices weiter. Erst Letztere interpretieren die Layout-Informationen und bearbeiten damit den IO-Request des pNFS-Client. Sie modifizieren auch selbstständig bei entsprechenden Schreibzugriffen auf eine Datei deren Layout und geben es an den pNFS-Client weiter. Der wiederum informiert den MSD mit der Operation *LAYOUTCOMMIT* über das neue Layout. pNFS-Clients können die Layouts aber auch über mehrere *OPEN*/*CLOSE*-Sequenzen hinweg zwischenspeichern.

Allerdings garantiert die Spezifikation dem pNFS-Client, dass im Falle einer anstehenden Layout-Modifikation durch einen anderen Client der MDS das Layout vor der Änderung per Callback *CB_LAYOUTRECALL* zurückfordert. Benötigt ein Client aus irgendeinem Grund das Layout einer Datei nicht mehr, gibt er es über die RPC-Operation *LAYOUTRETURN* gewissermaßen wieder frei.

Wenn Storage Devices als schlichte NFS-4-Fileserver agieren, kommt das **File-Layout** zum Einsatz. Es ist das einzige Speicherzugriffsprotokoll, dessen Beschreibung sich direkt im NFS-4.1-Standard [c] findet und dessen Spezifikation Netapp, Sun und IBM maßgeblich mitgestaltet haben.

Es enthält somit neben den Stripe-Größen, und -Lokationen (Storage Devices) auch

die NFS-Filehandles, die der Client für den Zugriff auf die einzelnen Dateibereiche verwenden muss. Das File-Layout ist kompakt und statisch, die Striping-Informationen ändern sich selbst bei Änderungen an der Datei nicht, sodass auch mehrere pNFS-Clients gleichzeitig das Layout zwischenspeichern können und kein Synchronisierungs-Overhead zwischen Clients und MDS beziehungsweise MDS und Storage Devices anfällt.

Dateisystemrechte und Clientauthentisierung lassen sich mit dem File-Layout sehr gut abbilden. Beim Einsatz von NFS 4 als Zugriffsprotokoll kommt es lediglich auf den verwendeten Security Flavor für die Client-Authentisierung an – bei Verwendung des Security Flavors *RPCSEC_GSS* erfolgt der Client-Zugriff beispielsweise kerberisiert; der Server setzt Zugriffsrechte also anhand gesetzter ACLs und über kryptografische Verfahren durch [2, 3].

Jenseits der Dateiorientierung

Hingegen verwendet das **Block/Volume-Layout** [d] – stark beeinflusst durch das von EMC für NAS-Heads entwickelte Multi-Path File System MPFS/MPFSi (früher als High Road bekannt) – Volume-Namen und Block-Offsets sowie -Extents zur Spezifikation des Layouts einer Datei. Der Zugriff auf die Storage Devices erfolgt demnach über die SCSI-Block-Kommandos. Da sich bei jedem schreibenden Zugriff auch die Blockverteilung ändern kann, muss das Layout häufiger aktualisiert werden als beim File-Layout. Meist beinhalten Virtualisierungskomponenten wie Volume Manager oder entsprechende Appliances konkrete Implementierungen, weil die Spezifikation eindeutige Volume-Namen zwingend vorschreibt.

Beim blockbasierten Zugriff auf die Storage Devices existiert keine wirklich sichere Authentisierungsmöglichkeit des SCSI-Initiators. Ein Zugriffsschutz im SAN erfolgt meist mit der Granularität ganzer Hosts, etwa auf Basis von World Wide Names (WWNs) bei Fibre Channel oder von Initiator Node Names (IQNs) bei iSCSI. Diese Grobgranularität stellt eine potenzielle Gefahr bei fehlerhaften oder böswilligen Clients dar. Abgesehen von der Frage clientseitiger Authentisierung, die lediglich iSCSI wenigstens bis zu einem gewissen Maß beantwortet, hat der Client entweder vollen Zugriff auf das Gerät oder ist komplett ausgesperrt. Die Einhaltung der per Dateisystem gewährten Zugriffsrechte setzt der Server nicht durch. Vielmehr hält sich ein pNFS-Client quasi freiwillig an die gewährten Rechte, das Storage Device muss dem pNFS-Client also vertrauen – eine grundsätzliche Schwäche der Zugriffskontrolle, das sich wie ein roter Faden durch die Geschichte des NFS-Protokolls zieht.

Syntaktisch ähnelt das **Object-Layout** [e] dem File-Layout. Es benutzt aber das SCSI Object Command Set für den Datenzugriff auf sogenannte Object-Based Storage Devices (OSDs) [f, g]. Bei deren Entwicklung ging es von Anfang um sichere Authentisierung und Zugriffskontrolle.

Die Sicherheit von OSDs beruht auf sogenannten Capabilities (Befähigungen) – ein Terminus, der in formalen Sicherheitsmodellen wohlbekannt ist. In diesen klassischen Subjekt-Objekt-Modellen ist eine Capability subjektgebunden und stellt ein authoritatives Zugriffsrecht auf ein Objekt oder eine Klasse von Objekten dar. Bei OSDs erfolgt der Datenzugriff unter Vorlage einer kyptografisch gesicherten Capability, die das Storage Device selbst überprüft. Das Object-Layout enthält diese Capability, sofern die dateibasierten Zugriffsrechte den gewünschten Zugriff erlauben. Anders ausgedrückt realisieren OSDs das klassische Referenzmonitor-Modell: die Policy wird in diesem Fall vom MDS – dem Referenzmonitor – definiert, den Mechanismus zur Durchsetzung („Enforcement“) legt aber das Storage Device fest. Änderungen an den ACLs (beispielsweise durch *chmod*-Kommandos oder Ähnliches) ziehen also stets Änderungen in den Objektstrukturen auf den OSDs nach sich.

pNFS ist erweiterbar für die spätere Einführung neuer Speicherzugriffsprotokolle, und Betriebssystem- und Storage-Herstellern steht es frei, zusätzliche Layout-Treiber für ihre pNFS-Implementierungen zu liefern. Abbildung 2 zeigt modellhaft eine exemplarische pNFS-Client-Implementierung.

Client-Fencing für den Fehlerfall

In einer Fehlersituation, beispielsweise dem Ausfall von Netzwerkleitungen, muss es zur Vermeidung von Datenkorruption möglich sein, einzelnen pNFS-Clients den Zugriff auf die Storage Devices dauerhaft zu verwehren (Fencing). Abgesehen von einer passenden Detektionslogik für diesen Fall kann beispielsweise der MDS bei Block/Volume-Layouts einen Zugriff

Neue Generation

NFS 4.1 erweitert den im April 2003 als RFC 3530 formulierten Standard NFS 4 um einige neue Eigenschaften, allen voran das parallele Dateisystem pNFS. Eine weitere wichtige Neuerung ist die Einführung sogenannter Sessions.

Eine Session ist ein vom Client dynamisch erzeugtes, persistentes Serverobjekt. Mit dessen Hilfe können Clients den Zustand einer NFS-Verbindung aufrechterhalten, egal ob diese gerade besteht oder nicht. Der Zustand überlebt daher auch zeitweilige Ausfälle sowohl des Servers als auch des Clients.

Jede Session hat einen sogenannten Fore Channel, die logische Verbindung vom Client zum Server für alle RPC-Operationen und optional einen Backchannel für RPC-Callbacks des Servers. Jedem Channel sind eine oder mehrere Transportverbindungen zugeordnet.

Damit lassen sich auch Callbacks durch Firewall-Grenzen hindurch realisieren, was bislang bei NFS 4 noch nicht in jedem Fall funktionierte.

Sessions erlauben unter anderem ein sogenanntes Trunking, sprich das Koppeln mehrerer physischer Transportverbindungen zwischen Client und Server zur selben Session, um den Datendurchsatz zu erhöhen. Neben diesem Session Trunking existiert noch das Client-ID Trunking, das mehrere Sessions zur selben Client-ID zusammenfasst.

Über Sessions realisiert NFS 4 erstmals auch eine sogenannte Exactly-Once-Semantik (EOS): Bislang half zwar ein meist implementierter, aber vollkommen unspezifizierter Reply Cache eines NFS-Server in einigen Fällen, mehrmals übertragene RPC-Operationen zu erkennen. Trotzdem war beispielsweise nach einem Neustart nicht auszuschließen, dass der NFS-Server nicht-idempotente Operationen wie *RENAME* mehrfach ausführte und damit sein Verhalten aus der Sicht des Clients unter Umständen nicht vorhersagbar war. NFS 4.1 fordert nun explizit einen Reply Cache, der persistent auf Platte liegt und die Server-Replies auf RPC-Operationen speichert.

Zu guter Letzt bieten Sessions eine erhöhte Sicherheit der RPC-Kommunikation, unter anderem durch das Einbinden von Callbacks in einen clientseitig vorgegebenen GSSAPI-Security-Context.

Neben einigen zusätzlichen RPC-Operationen ist als weitere Neuerung die Möglichkeit der Delegation für Verzeichnisse zu nennen. Bislang war Delegation nur für Dateien möglich.

auf die Management-Interfaces für das SAN besitzen, um ein entsprechendes LUN-Masking oder ein Zoning durchzuführen.

Bei der Verwendung von File-Layouts macht der MDS die Filehandles ungültig („invalidate“), die die pNFS-Clients besitzen, indem er die Storage Devices über das Kontrollprotokoll informiert. pNFS-Clients erhalten in diesem Fall den wohlbekannten Fehler „stale NFS handle“. In jedem Fall müssen Clients aber einen Timeout-basierten Fencing-Mechanismus für sich selbst bereitstellen.

Bei OSDs sieht das Sicherheitsmodell vor, dass das Storage Device beim Objektzugriff in der Capability des zugreifenden Clients das sogenannte Policy Access Tag mit dem Wert auf dem MDS vergleicht. Stimmen diese Werte nicht überein, verweigert es dem Client den Zugriff. Auf diese Weise lässt sich Fencing beim Object Layout realisieren.

Verfügbarkeit und Lastverteilung

Architekturseitig erlaubt pNFS den Einsatz mehrerer Metadatenserver, die sich über ein nicht näher spezifiziertes, durchaus auch herstellerabhängiges Kohärenzprotokoll abgleichen. Ein einzelner Client muss sich zwar per Mount an einen beliebigen, aber festen MDS binden, verschiedene Clients lassen sich dann aber wiederum auf verschiedene Metadatenserver verteilen – solange diese den selben globalen Namensraum exportieren und untereinander für eine Kohärenz der Layouts sorgen.

Eine zusätzliche Lastverteilung über mehrere Storage Devices funktioniert, wenn diese beispielsweise ein auf einem SAN lokalisiertes Cluster-Dateisystem per NFS 4 exportieren. Über das File-Layout kann der MDS die pNFS-Clients für den Datenzugriff an ein beliebiges Storage Device – also einen NFS-4-Server – verweisen. Das Layout selbst erzeugen die MDS dynamisch, um eine Lastverteilung oder eine Hochverfügbarkeit zu realisieren. Dazu müssen sie in der Lage sein, Ausfälle von Storage Devices zu erkennen und das Layout passend zu generieren. Darüber hinaus muss das Cluster-Dateisystem im Backend eine ausreichende Redundanz bieten (siehe Abbildung 3). Die pNFS-Spezifikation jedenfalls enthält in dieser Hinsicht keine Vorgaben.

Status und Ausblick

Derzeit sind die Arbeiten sowohl an einer Linux- als auch einer Opensolaris-Unterstützung für pNFS in vollem Gange. Für Linux existiert schon lange ein Prototyp mit dem parallelen Dateisystem PVFS2 (Parallel Virtual File System) als Speicherzugriffsprotokoll. PVFS2 [h] ist ebenfalls ein asymmetrisches, paralleles Dateisystem, das aber ein zum Zeitpunkt der Erstellung festgelegtes, sogenanntes algorithmisches Layout verwendet und daher einen relativ schlanken Overhead in der Kommunikation zwischen MDS und PVFS2-Servern aufweist. Der MDS stellt gleichzeitig einen PVFS2-Client dar und fungiert daher quasi als pNFS-PVFS2-Gateway. Mit dem Support von NFS 4 im Kernel unterstützt Linux auch das per Standard spezifizierte File-Layout – was maßgeblich der Arbeit von Netapp-Mitarbeitern, allen voran Trond Myklebust zu verdanken ist. Daneben existieren ein CITI-Projekt, um das Block-Layout für Linux zu implementieren [i] und ein Opensolaris-Projekt für die Unterstützung von OSDs [j].

Inzwischen haben namhafte Betriebssystem- und Storage-Hersteller wie EMC, Netapp, Panasas oder IBM den Inhalt von Draft 21 des geplanten NFS-4.1-Standards für den nächsten Bakeathon 2008 in Austin, Texas, fertiggestellt – ein traditionelles Event, auf dem Storage- und OS-Hersteller ihre NFS-Implementierungen gegeneinander auf Interoperabilität testen.

Im März 2008 steht das 71. IETF-Meeting in Philadelphia an, wo man mit Spannung verfolgen kann, ob NFS 4.1 und damit pNFS in den Status eines RFC (Request for Comments) erhoben wird, die nächste Entwicklungsstufe in Richtung eines vollwertigen Internet-Standards. (avr)

DR. OLIVER TENNERT

ist Head of Technology bei der Tübinger transtec AG.

Literatur

[1] D. A. Patterson, G. Gibson, R. Katz; A case for redundant arrays of inexpensive disks (RAID); Proceedings of the ACM SIGMOD International Conference on Management of Data; ACM 1988, S. 109-166

[2] Oliver Tennert; Filesysteme; Neue Datenwelten; Dateisystem fürs Netz: NFS Version 4; *iX* 5/2005, S. 118

[3] Oliver Tennert; Dateisysteme; An der Kette; Integrierte Sicherheit: NFS Version 4; *iX* 6/2005, S. 146

Onlinequellen

[a]	pNFS Problem Statement	www.pdl.cmu.edu/pNFS/
[b]	NASD: Network Attached Secure Disks	www.pdl.cmu.edu/NASD/index.html
[c]	NFS Version 4 Minor Version 1 draft 21	tools.ietf.org/html/draft-ietf-nfsv4-minorversion1-21
[d]	pNFS Block/Volume Layout draft 6	tools.ietf.org/html/draft-ietf-nfsv4-pnfs-block-06
[e]	Object-Based pNFS Operations draft 5	tools.ietf.org/html/draft-ietf-nfsv4-pnfs-obj-05
[f]	SCSI Object-Based Storage Device Commands (OSD) Working Draft	www.t10.org/ftp/t10/drafts/osd/osd-r10.pdf
[g]	SCSI Object-Based Storage Device Commands 2 (OSD-2) Working Draft	www.t10.org/ftp/t10/drafts/osd2/osd2r03.pdf
[h]	PVFS2 Homepage	www.pvfs.org
[i]	pNFS Block Layout for Linux	www.citi.umich.edu/projects/nfsv4/pnfs/block/
[j]	Object Storage Device (OSD) support for Solaris	opensolaris.org/os/project/osd/
[k]	NFSv4 Status Pages	tools.ietf.org/wg/nfsv4/
[l]	pNFS Informationsportal	www.pnfs.com
[m]	Opensolaris Project: NFS version 4.1 pNFS	opensolaris.org/os/project/nfsv41/
[n]	CITI Projects: ASC	www.citi.umich.edu/projects/asci/
[o]	Linux pNFS Kernel Development	www.citi.umich.edu/projects/asci/pnfs/linux/
[p]	Eislers NFS Blog	blogs.netapp.com/eislers_nfs_blog/
[q]	NFS 4.1. Bakeathon at Opensolaris.org	opensolaris.org/os/project/nfsv41/nfsv41_bakeathon/
[r]	EMC Celerra Multi-Path File System	www.emc.com/products/detail/software/celerra-multipath-file-system.htm

Sicherheitslücken in Anwendungen vorhersagen

Lückenhaft

Stephan Neuhaus, Andreas Zeller

Zum Vorhersagen von Sicherheitslücken reicht oft ein Blick in die Vergangenheit. Das Werkzeug „Vulture" durchkämmt die Fehlergeschichte eines Projekts, bildet die Lücken auf einzelne Komponenten ab und sagt für neue Komponenten voraus, wie wahrscheinlich Sicherheitslücken sind.

Dass Lücken in Software enorme Schäden verursachen, ist bekannt: Ein Bericht des FBI geht allein für 2005 von 67 Milliarden US-Dollar Schaden durch Computerkriminalität aus, das meiste davon durch schadhafte Software. Das Dilemma: Um Schaden abzuwenden, müsste man sich gezielt um kritische Komponenten kümmern, wenn man nur wüsste, welche das sind.

Eine Möglichkeit wäre, der Intuition des Programmierers zu vertrauen. Schreibt er beispielsweise an einer Web-Suite wie Mozilla, so weiß er, dass vermutlich der gesamte Bereich um Javascript verdächtig ist, denn dort traten schon häufig Sicherheitslücken auf. Mit dieser Methode lassen sich sicherlich einige besonders gefährdete Bereiche finden, aber nicht alle.

Eine bessere Lösung ist es, sich gezielt der Informationen zu bedienen, die während eines Softwareprojekts ohnehin anfallen: Versionsarchive und Fehlerdatenbanken. Wenn man die Informationen aus diesen beiden Quellen verknüpft, kann man genau herausfinden, wo Sicherheitslücken sind (siehe Kasten „Von Fehlerdatenbanken zu Sicherheitslücken"). Dieser Ansatz wurde im Werkzeug „Vulture" (englisch für „Geier") realisiert. Es entstand im Rahmen eines Forschungsprojektes an der Universität des Saarlandes.

Die Karte bringt es an den Tag

Wendet man Vulture beispielsweise auf die Web-Suite Mozilla an, entsteht eine Karte, wie sie in Abbildung 1 zu sehen ist. Diese Karte zeigt den kompletten Quellcode-Baum von Mozilla als Treemap. Rechtecke entsprechen Quellcode-Dateien beziehungsweise Verzeichnissen. Die Fläche eines Rechtecks ist dabei proportional zu seiner Größe. Quellcode-Dateien ohne Lücken sind dort weiß dargestellt. Dateien mit einer oder mehr Lücken haben einen mehr oder weniger starken Rotton: Je öfter in einer Datei eine Sicherheitslücke beseitigt werden musste, desto stärker ist sie rot gefärbt.

Auf der Karte erkennt man unten links einen stark rot gefärbten Bereich. Der gehört zum Verzeichnis „js", also dem Verzeichnis, in dem sich der Javascript-Interpreter befindet. Javascript scheint demnach in der Vergangenheit häufig zu Sicherheitslücken geführt zu haben, eine Beobachtung, die für Sicherheitsinteressierte nicht neu ist. Überraschender ist aber, dass auch ein anderer Bereich ziemlich rot ist: das darüber liegende Verzeichnis „layout". Anscheinend sind also auch diejenigen Teile von Mozilla anfällig für Lücken, die erst einmal nichts mit der Ausführung von Code zu tun haben.

Damit ist die Karte selbst schon wertvoll, weil sie ungeahnte Erkenntnisse über die Verteilung von Lücken im Quellcode liefert. Da das Verfahren außerdem völlig automatisch und ohne Rückgriff auf Intuition abläuft, gibt es dem Mozilla-Projekt ein Werkzeug an die Hand, mit dem die Beteiligten objektiv die Verteilung von Sicherheitslücken erkennen und damit die Aufteilung von Ressourcen auf die einzelnen Verzeichnisse oder Dateien planen können.

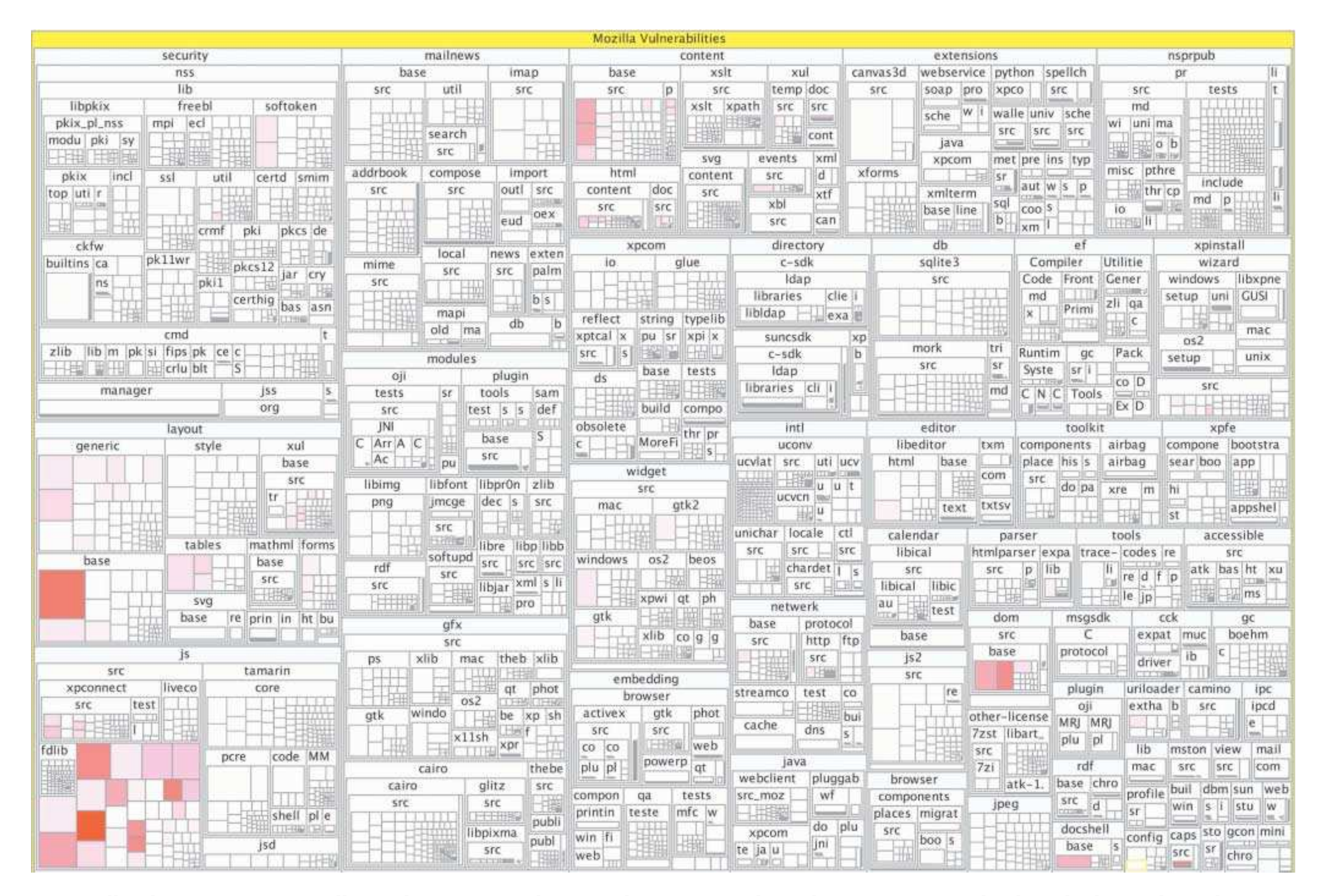
So eine Karte kann zudem jeder erstellen, der über ein Versionsarchiv und eine Bug-Datenbank verfügt und darüber hinaus eine Möglichkeit hat, unter den Bugs diejenigen zu identifizieren, die Lücken darstellen.

Ganz ohne Glaskugel

Allerdings möchte man nicht bei einer einfachen Beschreibung der vergangenen Lücken stehen bleiben, sondern stattdessen eine Möglichkeit haben, vorherzusagen, in welchen Dateien noch unentdeckte Fehler lauern.

Wie sieht das in der Praxis aus? Eine einfache Vorhersagemöglichkeit ergibt sich beispielsweise aus der Idee, dass Dateien, die in der Vergangenheit Lücken hatten, auch in Zukunft solche haben werden. Betrachtet man aber die tatsächlich Anzahl der Lücken pro Datei, erlebt man eine weitere Überraschung: Die meisten Dateien enthalten nämlich nur eine Lücke. Ihre Anzahl ist mehr als doppelt so groß wie die Anzahl der Dateien mit zwei oder mehr Lücken zusammengenommen (Abb. 2).

Man erwischt also mit einer solchen Vorhersage all diejenigen Dateien nicht, die nur



Im Quellcode-Baum von Mozilla sind Dateien und Verzeichnisse je nach Vorkommen von Sicherheitslücken schwächer oder stärker rot eingefärbt. Wenig überraschen die zahlreichen roten Flächen im Javascript-Bereich (js) links unten – diejenigen im darüberbefindlichen Verzeichnis „layout“ hingegen schon (Abb. 1).

einmal wegen einer Lücke geändert werden müssen. Da es sich dabei um mehr als zwei Drittel aller lückenhaften Dateien handelt, eignet sich die Anzahl der bisherigen Lücken pro Datei nicht zur Vorhersage.

Trotzdem ist die Idee der Vorhersage grundsätzlich Erfolg versprechend: Man sucht Eigenschaften von Dateien, die in der Vergangenheit mit Lücken zusammenhingen, und postuliert, dass das auch in Zukunft so sein wird.

Die Methode, aus Zusammenhängen, die in der Vergangenheit beobachtet wurden, auf zukünftige zu schließen, heißt „überwachtes Lernen“. Ist man beispielsweise überzeugt, dass lange Quellcode-Dateien für Lücken anfälliger sind als kurze, würde man etwa folgendermaßen vorgehen.

Zunächst werden Dateien aufgrund des Wissens, das die Vulture-Software liefert, in „lückenhaft“ und „(bisher) nicht lückenhaft“ eingeteilt. Außerdem ist die Länge der Quellcode-Dateien zu ermitteln. Dabei soll eine Maschine eine Funktion (auch „Modell“ genannt) so lernen, dass möglichst oft bei der Eingabe der Länge einer Datei richtig herauskommt, ob sie in der

Top 10 der betroffenen Include-Dateien

V und I	!V und I	Includes
19	0	*nsIEventListenerManager.h, nsIPresShell.h*
19	0	*nsReadableUtils.h, nsIPrivateDOMEvent.h*
15	0	*nsIScriptGlobalObject.h, nsDOMError.h*
14	0	*nsIScriptGlobalObject.h, nsDOMCID.h*
13	0	*nsIContent.h, nsIInterfaceRequestorUtils, nsContentUtils.h*
13	0	*nsISupportsPrimitives.h, nsContentUtils.h*
34	1	*nsCOMPtr, nsEventDispatcher.h*
29	1	*nsReadableUtils.h, nsGUIEvent.h*
22	1	*nsIScriptSecurityManager.h, nsIContent.h, nsContentUtils.h*
18	1	*nsWidgetsCID.h, nsContentUtils.h*

Die erste Spalte enthält die Anzahl der Dateien, die die mit Lücken assoziierten Include-Dateien aufweisen (I) und die in der Vergangenheit schon Lücken hatten (V). Die zweite Spalte enthält die Anzahl der Dateien, die diese Include-Dateien zwar aufweisen, aber keine Lücken hatten.

Top 10 der Vorhersagen

Rang	Komponente	verwundbar
1	*js/src/jsxdrapi*	*
2	*js/src/jsscope*	*
3	*modules/plugin/base/src/nsJSNPRuntime*	–
4	*js/src/jsatom*	–
5	*js/src/jsdate*	–
6	*cck/expat/xmlparse/xmlparse*	–
7	*layout/xul/base/src/nsSliderFrame*	*
8	*dom/src/base/nsJSUtils*	–
9	*layout/tables/nsTableRowFrame*	*
10	*layout/base/nsFrameManager*	*

In der Tabelle finden sich die vorhergesagten lückenhaften Quellcode-Dateien für Mozilla vom Januar 2007. Die letzte Spalte enthält ein „*“, wenn in der betreffenden Komponente bis zum Juli 2007 tatsächlich Lücken behoben werden mussten.

Vergangenheit verwundbar war oder nicht.

Um zu evaluieren, ob so ein Vorhersagemodell etwas taugt, wird nur mit einem Teil der möglichen Eingaben, der „Trainingsmenge“, gelernt und mit dem so erstellten Modell der andere Teil, die „Validierungsmenge“, vorhergesagt. Anhand der Vorhersagen und der tatsächlichen Ergebnisse für die Validierungsmenge kann man dann zählen, wie oft die Vorhersage mit der Wirklichkeit übereingestimmt hat.

Mit Modellen zur Vorhersage

Im genannten Beispiel würde man also zählen, wie oft das Modell korrekt vorhergesagt hat, ob eine Datei Lücken aufweist oder nicht. In der Praxis haben sich für solche Modelle zwei Gütemaßstäbe durchgesetzt:

– Der „Recall“ sagt aus, welcher Prozentsatz der lückenhaften Dateien korrekt als lückenhaft klassifiziert wurde.
– Die „Precision“ sagt aus, welcher Prozentsatz der als lückenhaft klassifizierten Dateien auch tatsächlich lückenhaft war.

Bei der Suche nach diesen Eigenschaften, die mit Lücken zusammenhängen, möchte man aufwendige Quellcode-Analysen möglichst vermeiden. Es stellte sich heraus, dass Include-Anweisungen und Funktionsaufrufe besonders gute Vorhersagen über Lücken erlauben. Include-Anweisungen sind Anweisungen für den C-Präprozessor. Dieser ist Teil des Übersetzungsvorgangs und wird vor dem Übersetzer aufgerufen.

Verdächtige Kandidaten

Include-Anweisungen bewirken, dass der Inhalt einer Datei (einer sogenannten „Header-Datei“) vor dem eigentlichen Übersetzungsvorgang an der angegebenen Stelle in den Quellcode einfügt wird. (Die C- beziehungsweise C++-Standards schreiben nicht vor, dass tatsächlich der Inhalt der Datei eingefügt wird, sondern besagen, dass das Ergebnis so sein soll, „als ob“ die Datei eingefügt worden wäre. Für das Projekt ist das ein zu vernachlässigender Unterschied.)

Welche Belege gibt es, dass Include-Anweisungen oder Funktionsaufrufe mit Lücken zusammenhängen? Betrachtet man einmal bei Mozilla diejenigen Dateien, die Include-Anweisungen sowohl für *nsIContent.h*, *nsIInterface RequestorUtils.h* als auch *nsContentUtils.h* enthalten, stellt man fest, dass diese 13 Dateien alle wegen Sicherheitslücken geändert werden mussten.

Ähnliches findet sich bei denjenigen Dateien, die Include-Anweisungen sowohl für *nsIScriptSecurityMana ger.h*, *nsIContent.h* als auch für *nsContentUtils.h* haben. Von diesen 23 Dateien hatten 22 in der Vergangenheit Lücken. Weitere Kandidaten sind in der Tabelle „Top 10 der betroffenen ...“ zu sehen.

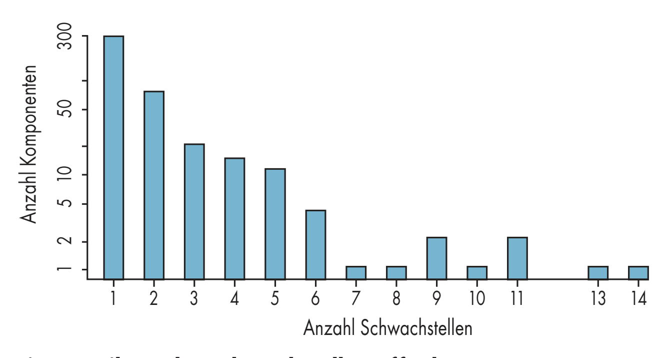
Die Zahlen sind äußerst beeindruckend, zeigen sie doch, dass es Kombinationen von Include-Dateien gibt, die sehr stark mit Lücken zusammenhängen. Dabei ist es tatsächlich die Kombination der Include-Dateien, die mit Lücken korreliert: Das bloße Einfügen von *nsReadable Utils.h* beispielsweise reicht nicht für das wahrscheinliche Vorhandensein einer Lücke, es muss noch *nsGUIEvent.h* oder *nsIPrivateDomEvent.h* dazukommen. Solche Zusammenhänge konnten im Projekt auch für Funktionsaufrufe beobachtet werden.

Ein großer Vorteil dieser Korrelation ist, dass man sie nicht einfach manipulieren kann. In der Vergangenheit führte das Entdecken solcher Korrelationen dazu, dass man Programmierern Ziele vorgab, die sie erfüllen mussten. Wurde beispielsweise beobachtet, dass größere Dateien in der Regel mehr Fehler haben als kleine, mussten sich die Programmierer an eine festgeschriebene Obergrenze für Dateigrößen halten. Die Folge waren aber nicht weniger

Von Fehlerdatenbanken zu Sicherheitslücken

Fehlerdatenbanken enthalten für jeden bekannten Fehler neben einer Beschreibung eine Fehlernummer, die diese Fehlerbeschreibung eindeutig benennt. Versionsarchive wiederum speichern die Änderungen an einem Softwareprojekt. Dazu gehören die geänderten Dateien und ein kurzer Text, der die Änderung beschreibt. Handelt es sich dabei um einen Bugfix, enthält der Text meistens auch die Fehlernummer als Bezug zu den Dateien, die geändert wurden, um den Bug zu fixen.

Jetzt gilt es nur noch herauszufinden, bei welchen Fehlernummern es sich um Sicherheitslücken handelt. Am leichtesten geht das, wenn wie beim Mozilla-Projekt eine Datenbank existiert, die zu jeder Lücke die davon betroffenen Fehlernummern ausweist. Auf diese Weise kommt man ausgehend von einer Sicherheitslücke an die Fehlernummern und zu den betroffenen Dateien.



Die Verteilung der Schwachstellen offenbart Unerwartetes: Die Anzahl der Dateien, die lediglich eine Sicherheitslücke enthalten, ist konkurrenzlos hoch (Abb. 2).

Fehler, sondern mehr kleine Dateien mit genauso vielen Fehlern. Will man aber etwas mit dem Mozilla Document Object Model anfangen, wird man in den meisten Fällen nicht darum herumkommen, die Include-Datei *nsDOMError.h* anzufordern. Ähnliches gilt für Funktionsaufrufe.

Wenn man nun aufgrund dieser Zusammenhänge die Verfahren des geschilderten maschinellen Lernens anwendet, geschieht etwas Interessantes: Das Verfahren klassifiziert einige Dateien als lückenhaft, für die bislang noch keine Lücken bekannt sind. Bedeutet das, dass das Verfahren fehlerhaft ist? Nein, es besagt, dass diese Dateien laut dem angewandten Verfahren eigentlich eine Lücke haben müssten, die jedoch noch nicht bekannt ist.

Die Autoren haben nun für Mozilla mit Stand vom Januar 2007 für alle Dateien, für die noch keine Lücken bekannt sind (das sind etwa 10 000) eine solche Vorhersage erstellen lassen und sie nach der Schwere der vorhergesagten Lückenhaftigkeit sortiert. Die Top 10 dieser Vorhersage zeigt die gleichnamige Tabelle. Das Sternchen in der letzten Spalte der Tabelle verrät, ob die Vorhersage zutraf oder nicht.

Software „Vulture"

Die Software ist grundsätzlich frei verfügbar. Sie besteht aus zwei Teilen: einem Teil, der die notwendigen Daten (Schwachstellen-Reports, Verknüpfung mit Softwarekomponenten) erhebt, und einem, der die statistischen Berechnungen erstellt.

Der erste Teil ist für jedes untersuchte Projekt anders und neu zu erstellen, deshalb wohl nicht für die Allgemeinheit interessant. Der zweite Teil besteht aus circa 500 Zeilen R-Skripten, die den im Artikel beschriebenen statistischen Ansatz auf sehr einfache Weise umsetzen.

Die Software wird zwar nicht zum Download angeboten, ist aber für Interessenten erhältlich. Kontakt über die Universität Saarbrücken oder die Redaktion.

Qualitätssicherung durch Vorhersage

In dem entsprechenden Zeitraum wurden in 55 bislang unbescholtenen Dateien Lücken behoben. Würde man Quellcode-Dateien zufällig auswählen, käme man auf eine Trefferquote von 55/10 000 = 0,55 % und in den Top 10 befände sich wahrscheinlich keine einzige lückenhafte Datei. Das angewandte Verfahren hat eine Trefferquote von 50 %. Hätten sich die Mozilla-Entwickler besonders auf diese Dateien konzentriert, hätten sie in jedem zweiten Fall eine oder mehrere Sicherheitslücken im Vorfeld stopfen können.

Das Projekt zeigt daher drei Dinge:

– Es gibt einen empirischen Zusammenhang zwischen Include-Dateien und Sicherheitslücken.

– Man kann dank dieses Zusammenhangs sehr gute Vorhersagen treffen, in welchen Dateien noch unbekannte Lücken sind.

– Quality-Assurance-Ressourcen kann man gemäß solcher Vorhersagen effektiv und effizient einsetzen.

Derzeit überträgt einer der Autoren gemeinsam mit einem Mitglied des Red-Hat-Security-Teams die Ergebnisse der Arbeit auf den Red-Hat-Code, mit ersten positiven Ergebnissen. (ur)

ANDREAS ZELLER

ist Professor für Softwaretechnik an der Universität des Saarlandes in Saarbrücken und Autor des Buches „Why Programs Fail – A Guide to Systematic Debugging". Sein Forschungsgebiet ist die Analyse großer Softwaresysteme und deren Fehler.

DR. STEPHAN NEUHAUS

ist Geschäftsführer der Sasecure Computersicherheit GmbH in Saarbrücken. Er beschäftigt sich schon seit 1992 mit Computersicherheit.

Literatur

[1] Stephan Neuhaus, Thomas Zimmermann, Christian Holler, Andreas Zeller; Predicting Vulnerable Software Components. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS); October 2007, S. 529–540



Umgang mit häufigen Änderungen in XSD-Schemata

E-Skulapstab

Axel Benz, Heike Schwarz, Manuel Aldana

Wenn XSD-Schemata als Schnittstellenbeschreibungen häufigen Änderungen unterworfen sind, wächst der Pflegeaufwand in der Softwareentwicklung stark. Allerdings nicht zwingend, wie ein Projekt aus dem Umfeld der geplanten Gesundheitskarte zeigt.

Modellgetriebene Softwareentwicklung ist großartig, weil bei einer Änderung des Modells ein Knopfdruck alle Schnittstellen neu generiert. Deshalb denken Architekten, dass man Änderungen des Modells im Griff hat, weswegen es häufig Änderungen gibt. Schlimmer noch: Mehrere Versionen der Schnittstellen können parallel existieren und müssen bedient werden. Ausbaden dürfen das die Entwickler.

Was die Änderung eines über XML-Schemata (nach dem W3C-Standard www.w3.org/XML/Schema, meist schlicht als XSD bezeichnet) implementierten Datenmodells für den bedeutet, der die Daten lesen und schreiben soll, kommt auf die Datenhaltung an. Zwei Varianten stehen zur Auswahl: die dynamische Datenhaltung in einem Document Object Model (DOM) und die statische durch XML Binding.

Daten in einem DOM-Objekt zu halten, ist weniger beliebt, da die Performanz als kritisch gilt und vor allem die Typsicherheit nicht gewährleistet ist. So kann man beispielsweise beliebige Tags anhängen, was Java-Programmierer nicht mögen. Deswegen dürften Entwickler eher ein XML Binding (mit einer JAXB-Implementierung für Java oder dem XML Schema Definition Tool für .Net) verwenden.

Bindings versus modellgetrieben

Ein Projekt in diesem Umfeld, die Spezifikation der Telematikinfrastruktur der elektronischen Gesundheitskarte, hat die Gematik GmbH im Auftrag des Bundesgesundheitsministeriums umgesetzt. Die Datenstrukturen der medizinischen Objekte werden als XSD-Schemata modellgetrieben aus UML generiert.

Hinter solch einer Datenstruktur verbirgt sich beispielsweise das elektronische Rezept. Wenn ein Arzt ein E-Rezept erstellt und ein Patient es in der Apotheke einlösen können soll, sind folgende Schritte notwendig:

– Der Arzt füllt das GUI seines Praxisinformationssystems mit den Inhalten des Rezeptes.
– Aus den Inhalten erzeugt Software eine schemakonforme XML-Datei, die über die Telematik-Infrastuktur sicher zur Apotheke gelangt.
– In der Apotheke validiert ein Programm die XML-Daten gegen das passende Schema, liest sie aus und zeigt sie im Apothekeninformationssystem an.
– Im Apothekeninformationssystem werden die Abrechnungsdaten ausgefüllt und die XML-Daten mit ihnen schemakonform ergänzt.
– Schließlich leitet die Software die XML-Daten zum Abrechnungssystem der Versicherungen weiter.

Abbildung 1 zeigt den Vorgang übersichtlicher. Das Rezept-Schema hat eine Tiefe von 22 Knoten und sprechende Knotennamen. So ist, um die Einheit der Wirkstoffmenge (Milligramm oder Gramm) zu lesen, ein XML-Binding-Objekt beispielsweise folgendermaßen anzusprechen:

```
getUC_eVerordnungXML().get↵
    EVerordnung().getArzneimittel↵
Verordnung().getFertigarzneimittel().↵
    getPackungsmenge().get↵
PackungsgroesseNachAbgeteilter↵
    Menge().getEinheit()
```

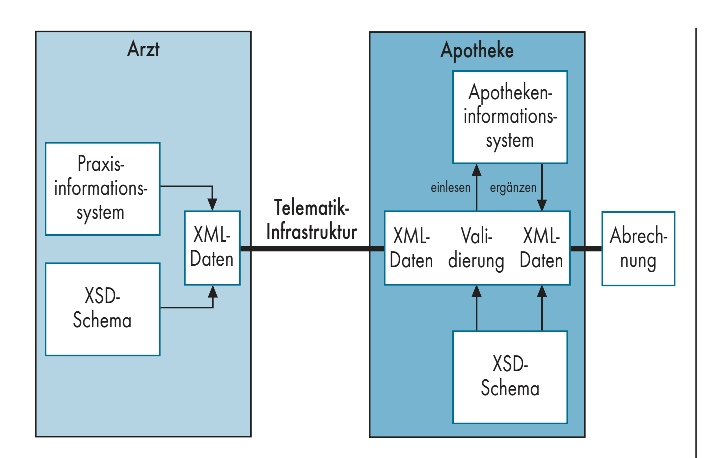
Wenn sich das Modell ändert – wenn etwa die Ebene *PackungsgroesseNachAbgeteilterMenge* entfällt –, erfordert das Modifikationen an jeder Stelle, an der ein Programm lesend oder schreibend auf die Daten zugreift. Man könnte dies durch einen geeigneten Wrapper erreichen, der einen einheitlichen Zugriff anbietet. Beispielsweise könnte *setEinheit()* die Einheit setzen, gleichgültig an welcher Position das Element tatsächlich in der XSD auftaucht. Den Wrapper muss man allerdings nach jeder Schemaänderung neu schreiben, was aufwendig, repetitiv, langweilig und daher fehleranfällig ist. Eine weitere kritische Situation tritt ein, wenn es gilt, zwei Versionen der Schnittstelle gleichzeitig zu bedienen.

Es ist zweimal fast (aber nur fast) identischer Code für das Binding zu generieren – der generierte Code explodiert, was unter anderem zu Unübersichtlichkeit bei der Typadressierung führt: Viele ähnliche Typen stehen in den *import*-Anweisungen, lange Paketnamen sind im Source-Code verstreut. Beim Einlesen von XML-Daten muss das Schema bekannt sein. Da die Schemaversion aber in den XML-Daten steht, beißt sich die Katze in den Schwanz. Es bleibt nur übrig, auszuprobieren, in welches Binding-Objekt die Daten passen.

Leider ist das kein guter Programmierstil, folglich muss man den Namensraum aus den XML-Daten lesen. In diesem Fall muss Software das XML aber zunächst analysieren (Parsing) – vielleicht über ein DOM? Da wäre es wohl besser, die Daten gleich in einem DOM zu halten.

Das DOM reicht nicht aus

Wer auf eine Überprüfung der Typsicherheit zur Entwicklungszeit verzichtet, kann die Daten in ein DOM-Objekt einlesen und zur Laufzeit gegen das Schema validieren.



Vom Arzt in die Apotheke und weiter zur Krankenkasse: der Weg der XML-Daten (Abb. 1)

Hierzu müssen die Daten als XML vorliegen, was allerdings nicht immer der Fall ist. So muss beispielsweise bei der Erzeugung eines neuen elektronischen Rezepts Software die ganze Datenstruktur Element für Element aufbauen. Soll sie in einen optionalen Zweig der Datenstruktur schreiben, der noch nicht existiert, muss sie zunächst diesen Zweig schemagerecht inklusive Namensraumpräfixen, Attributen et cetera konstruieren. Daher ist es sinnvoll, die Schnittstelle zum DOM zu erweitern.

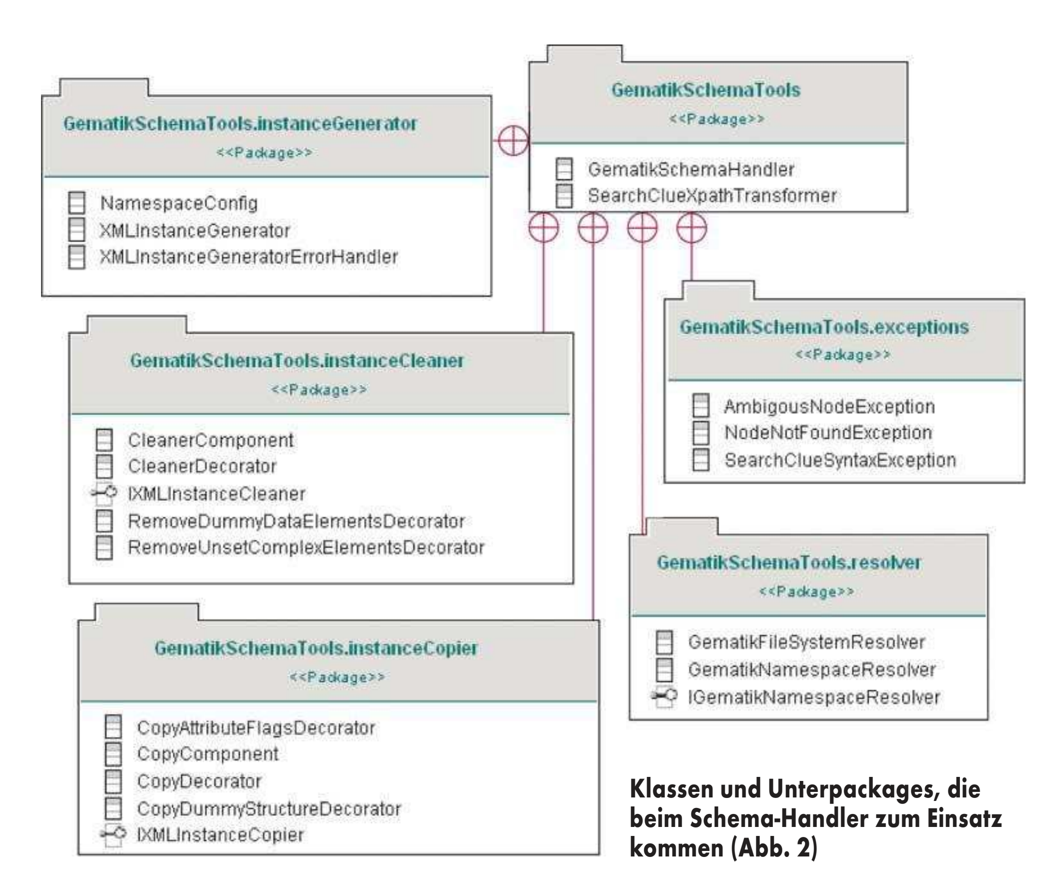
Die Artefakte der modellgetriebenen Softwareentwicklung sind bei genauerem Hinsehen nicht so unhandlich wie oben dargestellt. Folgende Randbedingungen können genutzt werden: Die Namen der Blattelemente der Schnittstellen sind meistens eindeutig und ändern sich selten. Änderungen beziehen sich in der Regel auf die innere Struktur der Schemas, oder es handelt sich um dessen einfache Erweiterung.

Diese Randbedingungen kann man nutzen, um Code zu entwickeln, der gegen Schemaänderungen robust ist. Der Schlüssel hierzu ist XPath, das XML-Elemente anspricht. Wenn die Namen der Blattelemente eindeutig sind, reicht ein einfacher XPath-Ausdruck zur Identifikation des zu lesenden oder zu schreibenden Knotens. Dieser Ausdruck ändert sich nicht, wenn sich nur die innere Struktur des Schemas ändert. Bei uneindeutigen Blattelementen kann ein minimaler XPath-Ausdruck dazu dienen, nur die nötigen Knoten auf dem Weg von der Wurzel zum Blatt herauszusuchen; er ist damit robust gegen Schemaänderungen.

Vom Arzt zur Apotheke

Bei der von der Gematik implementierten Lösung handelt es sich um eine Komponente, mit der sich über XPath Knoten einer XML-Datenstruktur identifizieren und lesen oder schreiben lassen. Im Unterschied zum DOM generiert sie beim Schreiben automatisch fehlende Teilbäume und alle Attribute des XML. Mit den folgenden Funktionen lässt sich die oben beschriebene Übergabe von XML-Daten zwischen Arzt und Apotheke komfortabel realisieren.

Der Konstruktor des Schema-Handlers bekommt die XSD-Information als String, URL oder Document mitgeliefert, damit er wissen kann, wie fehlende Teilbäume aufzubauen sind. Weiterhin muss eine Abbildung zwischen Namensraum und Schema-Ablage erfolgen. Dies geschieht über die Schnittstelle *GematikNamespaceResolver*. Die Implementierung dieser



Klassen und Unterpackages, die beim Schema-Handler zum Einsatz kommen (Abb. 2)

Schnittstelle entscheidet, ob die Abbildung auf eine HTTP-Resource (online) oder ein lokales XSD-Repository im Dateisystem (offline) erfolgt:

```
GematikSchemaHandler(String|⁊
    Document|URL xsd,⁊
    GematikNamespaceResolver ⁊
    namespaceResolver)
```

Dieser Konstruktor erzeugt automatisch ein DOM-Objekt, dessen Blattknoten zunächst mit Werten gefüllt sind, die als „uninitialisiert“ erkennbar sind. Das DOM-Objekt enthält alle optionalen Elemente und alle Zweige von Choices, sodass es in diesem Zustand noch nicht valide sein kann. Die uninitialisierten Blätter können nun mit Werten – beispielsweise den Inhalten des E-Rezeptes – gefüllt werden. Hierzu dienen die Methoden

```
setNodeValue(String newText,
    String... searchClues)
setNodeValue(String newText, XPath
    xpath)
```

SearchClues bezeichnet eine Reihe von Elementnamen, die einen eindeutigen Pfad zum Knoten darstellen. Intern erfolgt eine Transformierung zwischen *SearchClue* und XPath. So kann man selbst ohne XPath-Kenntnisse Knoten ansprechen. Dies ist hilfreich, da XPath-Ausdrücke bezogen auf Erstellung und Lesbarkeit nicht gerade einfach zu handhaben sind. Falls der gesetzte Wert auf einem Zweig eines Choice liegt, werden automatisch alle anderen Zweige gelöscht.

Nach der *setNodeValue()*-Operation sind noch die uninitialisierten optionalen Elemente und nicht gesetzten Attribute zu entfernen. Hierzu dient die Methode *cleanupXmlDocument()* Da die uninitialisierten Elemente als solche erkennbar sind, stellt sich das Entfernen als einfach dar. Allerdings muss man darauf achten, dass gelegentlich ganze Zweige optional sein können und wegfallen müssen. Nun sollte ein schemakonformes DOM-Objekt vorliegen, was sich mit der Methode *ValidationResult validateXmlDocument()* prüfen lässt. Eine Validierung, die nur *true* oder *false* als Ergebnis hat, dürfte den Benutzer nicht erhellen – vor allem wenn das Ergebnis *false* ist. Deswegen enthält *ValidationResult* eine detaillierte Fehlernachricht über das Ergebnis. Hierzu dienen die Methoden:

```
String getValidationMessage()
boolean isValidationSuccessfull()
```

Das DOM-Objekt lässt sich nun mit der Methode *get XML()* in einen XML-String serialisieren und an die Apotheke übertragen, die wiederum das E-Rezept in Form von XML-Daten erhält. Beim Aufbau des Schema-Handler-Objekts liest der Resolver den Namensraum aus den XML-Daten und wählt das passende Schema aus. Aus dem resultierenden Objekt kann man schon Werte auslesen. Hierzu steht als Gegenstück zu *setNodeValue* die Methode *String getNodeValue(String…searchClues)* zur Verfügung. Validierung und Hinzufügen von Abrechnungsdaten können dann genauso erfolgen wie beim initialen Einlesen von Daten beim Arzt.

Die einzelnen Komponenten des Schema-Handlers sind in einem Package *Gematik Schema Tools* zusammengefasst. Dessen Klassen und Unterpackages spiegeln die Aufgaben wieder, die beim Schema-Handler zum Einsatz kommen: Der Instanzgenerator erzeugt aus den Schemata XML-Instanzen. Undefinierte Elemente löscht der Instanz-Cleaner aus einer XML-Instanz. Der Instanz-Copier führt XML-Teilbäume zusammen, und der Resolver bildet Namensräume auf die XSD-Ablage ab (siehe Abbildung 2).

Bei den Referenzimplementierungen der meisten Komponenten der Gesundheitstelematik, wie sie die Gematik erstellt, kommt der Schema Handler an verschiedenen Stellen zum Einsatz. Die bisherigen Erfahrungen sind gut. Die Befürchtung, dass die Verwendung des Schema-Handlers anstelle von XML-Bindings einen Performance-Engpass hervorrufen würde, hat sich bisher nicht bewahrheitet. (hb)

PROF. DR. AXEL BENZ

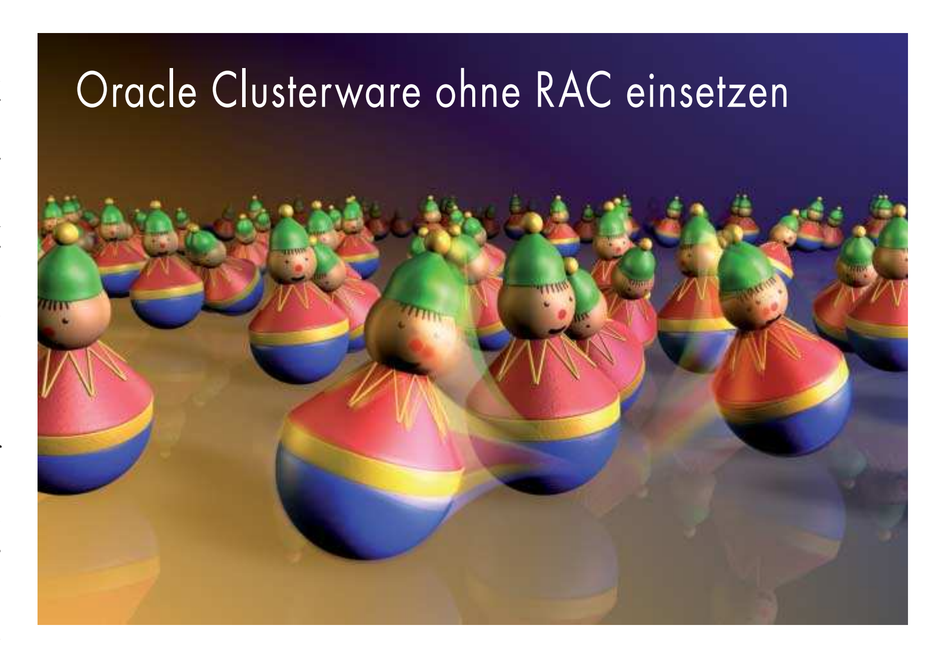
war bis April 2007 Leiter des Bereichs Entwicklung der Gematik GmbH. Heute lehrt er Systementwicklung an der Fachhochschule für Wirtschaft, Berlin.

DIPL.-INFORM. HEIKE SCHWARZ

ist innerhalb der Entwicklungsabteilung der Gematik GmbH für den Bereich .Net-Entwicklung zuständig.

DIPL.-INFORM. MANUEL ALDANA

ist Software-Ingenieur bei der Gematik GmbH mit dem Schwerpunkt Softwarewartung, -qualität und -design.



Im Takt

Martin Bach

Oracles Cluster-Infrastruktur eignet sich nicht nur zum unterbrechungsfreien Betrieb von Datenbanken. Auch andere Server lassen sich mit ihr so im Cluster einsetzen, dass sie rund um die Uhr zur Verfügung stehen.

Hochverfügbarkeit ist in aller Munde: Applikationen, Datenbanken und Infrastruktur müssen immer und jederzeit arbeiten, und sogar kleinere Unternehmen stehen oft vor der Aufgabe, ihre Anwendungen ununterbrochen bereitzustellen. Oracle bietet dafür seinen Real Application Cluster (RAC) an. Das zugrunde liegende Cluster Framework lässt sich aber auch alleine verwenden – ohne separate RAC-Lizenz. Damit lassen sich beliebige Anwendungen absichern.

Im folgenden Praxisartikel soll es darum gehen, den Apache-Webserver auf einem Cluster aus zwei Knoten mithilfe von Clusterware zu betreiben. Sofern man einige Voraussetzungen beachtet, ist das Installieren der Software unkompliziert. Auf otn.oracle.com stehen Clusterware 10.2 und 11 für alle wichtigen Betriebssysteme zum Download zur Verfügung, die Datenbanksoftware ist nicht erforderlich. Im Weiteren geht es um die Clusterware 11g für 64-Bit-Linux. Als Betriebssystem kommt Red Hat Enterprise Linux 5 mit Update 1 zum Einsatz, jeder seiner Clone (CentOS/Oracle Enterprise Linux) sollte es genauso tun. Auf größere Unterschiede zwischen Clusterware 10.2.x und 11.1.x geht der Text gegebenenfalls ein. Für Clusterware 10.2.x auf Red Hat 5 sind Anpassungen an zwei Dateien durchzuführen (*./install/oraparam.ini* und *./stage/prereq/crs/refhost.xml*), damit das Installationsprogramm die Systemvoraussetzungen prüfen kann. Details zu diesen Änderungen führen Metalink Note 421308.1 und 456634.1 auf. Alternativ lässt sich der Installer mit *./runInstaller -ignoreSysPrereqs* starten, was die Prüfungen bezüglich Betriebssystem und notwendiger RPMs komplett unterdrückt.

Clusterware bedient sich zweier von allen Knoten genutzten Dateien zur Verwaltung: der Voting Disk und der Oracle Cluster Registry (OCR). Sie müssen bei der Standard-Edition zwingend auf Raw Devices liegen, die Enterprise-Edition lässt auch das Cluster-Dateisystem OCFS2 oder NAS zu. Vorsicht aber bei NFS: es sind bei Weitem nicht alle NAS-Appliances zertifiziert, zudem müssen einige Optionen in der */etc/fstab* stehen, damit Clusterware mit NFS fehlerfrei arbeiten kann. Für Geräte von Netapp zum Beispiel sind folgende Mount-Optionen für OCR und Voting Disk zu setzen:

```
nas_appliance:/nfs_volume /oracle/crs/shared \
  nfs hard,nointr,proto=tcp,suid,vers=3,rw,bg,\
  rsize=32768,wsize=32768,actimeo=0,timeo=600
```

Neben OCR und Voting Disk sind zwei separate physische Netze notwendig. Das erste („öffentliche“) stellt die Verbindung zur Außenwelt her und erlaubt eingehende Verbindungen. Das zweite („private“) ist für interne Zwecke von Clusterware reserviert. Da keine Crossover-Kabel erlaubt sind, müssen schnelle Switches her.

Virtuelle Adresse migriert beim Ausfall

Um langes Warten auf TCP-Timeouts zu vermeiden, erzeugt und verwaltet Clusterware dem öffentlichen Netz-Interface zugeordnete virtuelle IP-Adressen (Aliase). Im Fehlerfall kann die virtuelle IP (kurz VIP) von dem nicht mehr verfügbaren Server auf einen der übriggebliebenen migrieren. Alle Anfragen an sie beantwortet der Kernel dann mit einem NACK, und der Timeout ist vermieden. Die IP-Adressen dieser virtuellen Interfaces müssen Teil des öffentlichen Netzes sein, dürfen logischerweise keinem anderen Host zugewiesen sein und werden während der Installation von Clusterware initialisiert.

Zusätzlich zu diesen bereits seit 10.1.x bekannten virtuellen IP-Adressen, die hauptsächlich für RAC-Datenbanken zum Einsatz kommen, gibt es seit 10.2 sogenannte Application VIPs. Sie sind im Gegensatz zur klassischen VIP immer nur auf einem Knoten aktiv und ähneln Veritas' Floating IPs. Das Beispiel konfiguriert den Apache so, dass er unter einer solchen Application VIP im öffentlichen Netz erreichbar ist.

Da keine weitergehende RAC-Installation folgt, kann man Clusterware unter einem beliebigen Account einrichten, sofern er *oinstall* als primäre Gruppe hat. Der Einfachheit halber sei hier *oracle* für diesen Zweck gewählt.

Alle Rechner des Clusters müssen Voting Disk und OCR anbinden, damit sie die Integrität des Clusters gewährleisten können. Liegen diese beiden auf Raw Devices, ist ab Red Hat 5 die Verwendung von *udev* notwendig, */etc/sysconfig/rawdevices* existiert nicht mehr.

Listing 1: Einträge in /etc/hosts

```
# 1) öffentliches Netz

# 1.1) Physische Adressen - eth0

192.168.17.100     node1.localdomain         node1
192.168.17.200     node2.localdomain         node2

# 1.2) Virtuelle Adressen, basierend auf eth0

192.168.17.101     node1-vip.localdomain        node1-vip     # Clusterware-intern
192.168.17.201     node2-vip.localdomain        node2-vip     # Clusterware-intern
192.168.17.130     floating_vip.localdomain     floating-vip  # für Apache

# 2) privates Netz - eth1

192.168.0.100     node1-priv.localdomain        node1-priv
192.168.0.200     node2-priv.localdomain        node2-priv
```

Die notwendigen Anpassungen sind in */etc/udev/rules.d/60-raw.rules* zu erledigen; ein Beispiel könnte so aussehen:

```
ACTION=="add", KERNEL=="sdb1", \
  RUN+="/bin/raw /dev/raw/raw1 %N"
ACTION=="add", KERNEL=="sdb2", \
  RUN+="/bin/raw /dev/raw/raw2 %N"
KERNEL=="raw[0-9]*", OWNER="oracle", \
  GROUP="oinstall", MODE="640"
```

Diese Einträge machen dem Betriebssystem auf beiden Knoten */dev/sdb1* als */dev/raw/raw1* und */dev/sdb2* als */dev/raw/raw2* bekannt. Außerdem ordnen sie alle Raw Devices dem Account *oracle* mit der Gruppe *oinstall* zu und setzen die Rechte auf *rw-rw--*. Zu diesem Thema gibt es bei Metalink weitergehende Informationen, siehe Note 414897.1. Obwohl die Verwendung von *udev* mit Red Hat 4/SLES 9 nicht zwingend notwendig ist, sei es auch dort dringend angeraten.

Drei Arten von IP-Adressen

Sicherheitshalber sollten sich die Mitglieder des Clusters gegenseitig in */etc/hosts* mit ihren öffentlichen, privaten und virtuellen IP-Adressen eintragen. Ein Beispiel dafür zeigt Listing 1.

Für die Inbetriebnahme von Clusterware ist es zudem notwendig, SSH-Schlüsselpaare (RSA und DSA) zu erzeugen und ihre öffentlichen Teile jeweils auf der Gegenseite in *~oracle/.ssh/authorized_keys* einzutragen.

Sicherheitsbewusste Administratoren haben oftmals SELinux und *iptables* auf ihren Servern konfiguriert – an dieser Stelle sei für erforderliche Anpassungen auf Metalink hingewiesen. Um das Beispiel nicht unnötig zu komplizieren, seien SELinux und die Firewall deaktiviert.

Da Clusterware tief in das System eingreift, sind einige Parameter in */etc/sysctl.conf* erforderlich (siehe Listing 2). Sind alle diese Schritte erledigt, sollte die Einrichtung anstandslos durchlaufen. Den nervigen Fehler in Version 10.2.0.1 („Could not find a suitable set of interfaces for VIPs“) hat 11g endlich behoben. Den Workaround für den Vorgänger – manuelles Starten des „vip configuration assistant“ *vipca* – beschreiben Metalink Note 338924.1 und viele Blogs.

Listing 2: Einträge in /etc/sysctl.conf

```
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
net.core.rmem_default = 262144
net.core.rmem_max = 4194304
net.core.wmem_default = 262144
net.core.wmem_max = 262144
```

Sofern noch nicht geschehen, sollte *ORA_CRS_HOME* in */root/.bashrc* und *~oracle/.bashrc* eingetragen und definiert werden, zudem sollte die *PATH*-Umgebungsvariable um *$ORA_CRS_HOME/bin* ergänzt werden. *$ORA_CRS_HOME/bin/crs_stat -t* sollte nach erfolgreicher Installation diese Ausgabe liefern:

```
Name           Type          Target    State     Host
------------------------------------------------------
ora.node1.gsd  application   ONLINE    ONLINE    node1
ora.node1.ons  application   ONLINE    ONLINE    node1
ora.node1.vip  application   ONLINE    ONLINE    node1
ora.node2.gsd  application   ONLINE    ONLINE    node2
ora.node2.ons  application   ONLINE    ONLINE    node2
ora.node2.vip  application   ONLINE    ONLINE    node2
```

Die aufgeführten Ressourcen werden standardmäßig während der Softwareinstallation angelegt und initialisiert. GSD ist der Global Service Daemon, ONS der Oracle Notification Service. Die VIP-Ressource ist für die virtuellen IP-Adressen zuständig. Es ist wichtig, dass sich alle Ressourcen im Status „ONLINE“ befinden.

Um Apache mit Clusterware abzusichern, braucht man eine „floating IP“, die im Fehlerfall vom ausgefallenen zum funktionsfähigen Knoten wandern kann, ohne dass der Client das bemerkt. In Oracles Terminologie heißt eine solche IP-Adresse „Application VIP“. Sie zu erstellen ist relativ einfach; auf dem ersten Knoten als *root* angemeldet, erledigt das dieser Aufruf von *crs_profile*:

```
crs_profile -create floating_vip \
  -t application -a $ORA_CRS_HOME/bin/usrvip \
  -o oi=eth0,ov=192.168.17.130,on=255.255.255.0
```

crs_profile ist zuständig für die Definition eines „Profils“, das die Interaktion zwischen dem Clusterware-Framework und der von ihm verwalteten Ressource regelt. Das Beispiel erzeugt die neue Ressource *floating_vip* vom Typ *application*. *$ORA_CRS_HOME/bin/usrvip* gehört zum Lieferumfang von Clusterware und kümmert sich um die interne Verwaltung des virtuellen Interface.

IP-Adresse auf Wanderschaft

Anwender rufen *usrvip* nicht auf, um das Interface zu steuern. Das erledigen vielmehr die Programme *crs_start*, *crs_stop* und *crs_relocate*. Die per *-o* übergebenen Optionen legen das Interface (*oi*), die IP-Adresse des Apache (*ov*) und die zugehörige Netzmaske (*on*) fest.

crs_profile erzeugt eine sogenannte CAP-Datei, die *crs_register floating_vip* in die Cluster Registry einträgt. *crs_setperm* ist dafür zuständig, anderen Benutzern Kontrolle über diese Ressource zu geben. Im Beispiel soll sie der Benutzer *oracle* verwalten können:

```
crs_setperm floating_vip -u user:oracle:r-x
```

Ein erneuter Aufruf von *crs_stat -t* liefert nun:

```
Name           Type          Target    State     Host
------------------------------------------------------
floating_vip   application   OFFLINE   OFFLINE
ora.node1.gsd  application   ONLINE    ONLINE    node1
...            ...           ...
```

crs_stat -p <Ressource> informiert über die Profile einer Ressource, *-ls* über die Rechte.

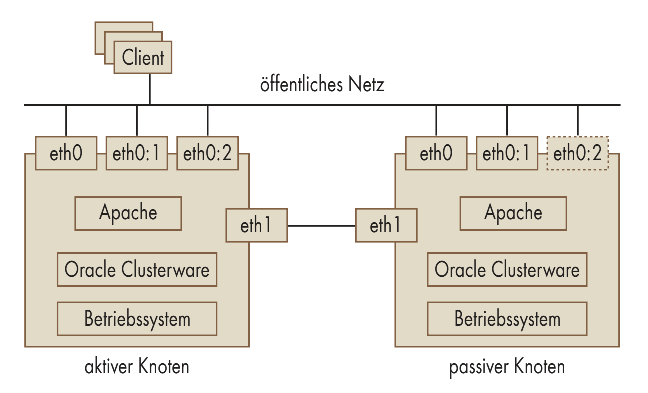
Der Benutzer *oracle* kann nun das virtuelle Interface starten:

```
crs_start floating_vip
```

crs_stat -t zeigt jetzt *floating_vip* als „ONLINE“ auf node1, und *ifconfig* gibt eine weitere Adresse aus, *eth0:2*:

```
eth0:2   Link encap:Ethernet ...
...      inet addr:192.168.17.130 ...
```

Für Apache ist dasselbe Vorgehen notwendig: Erzeugen und Registrieren des



Legende

eth0: erste physikalische Netzwerkkarte
eth0:1 virtuelle IP-Adresse (Clusterware)
eth0:2 floating_vip, ebenso virtuelles Interface
eth1: zweite physische Netzwerkkarte
gestrichelte Linien bedeuten inaktive Komponenten

Profils, Rechte zuweisen und anschließendes Starten der Ressource. Der Unterschied zum Erzeugen von *floating_vip* besteht darin, dass ein kleines Programm nötig ist, das die Ressource „Apache" verwaltet. Das Clusterware-Framework schreibt vor, dass dieses Skript oder Programm drei Funktionen ausführen kann: *start()*, *stop()* und *check()*.

Starten und Anhalten auf neue Art

Ein Template für ein solches Skript findet sich unter *$ORA_CRS_HOME/crs/public/action_scr.scr*. Für Apache verwendet das Beispiel *apachectl* zum Starten und Beenden, ein simples *ps -ef | grep httpd* prüft, ob Apache-Prozesse aktiv sind (Exit-Code 1) oder nicht (Exit-Code 0). Dies steht im Kontrast zur Unix-Tradition, in der 0 Erfolg signalisiert.

Am einfachsten ist es, als *root* das Template umzubenennen und an den relevanten Stellen anzupassen. Danach sollte man es als *$ORA_CRS_HOME/crs/script/apache.scr* speichern. *chmod 750* setzt die notwendigen Rechte. Es empfiehlt sich außerdem ein Test, zum Beispiel mit *./apache.scr start*. Funktioniert alles wie gewünscht, kopiert man es auf den zweiten Knoten in das gleiche Verzeichnis, am einfachsten mittels *scp*.

Wie bei der Application VIP erfolgt die Registrierung des Scripts in Clusterware in zwei Schritten: *crs_profile* erzeugt das Profil (die CAP-Datei), und *crs_register* trägt es in die Cluster Registry ein.

```
crs_profile -create apache -t application \
-d "Apache Server" -r floating_vip \
-a apache.scr -o ci=30,ft=3,fi=12,ra=5
```

-create erzeugt die Ressource vom Typ *application*, die von *floating_ip* abhängt (*-r*). Das zugehörige Script ist *apache.scr* (*-a*) in *$ORA_CRS_HOME/crs*. Die Kette von Optionen (*-o*) instruiert Clusterware, alle 30 Sekunden (*ci=30*) den Apache-Status zu prüfen, aber erst nach dem dritten Fehler in Folge die Anwendung als nicht verfügbar zu erkennen (*ft=3*). Nach der erfolglosen Prüfung soll Clusterware versuchen, alle 12 Sekunden (*fi=12*) den Status zu ermitteln. Scheitert es damit zum fünften Mal (*ra=5*), startet es Apache auf dem zweiten Knoten.

Nach dem Erstellen des Profils registriert *crs_register apache* das Ganze in der Cluster Registry. Nun kann *crs_start apache* die Ressource starten. Eine Überprüfung mit *crs_stat -t* ergibt:

```
Name          Type         Target    State     Host
-----------------------------------------------------
apache        application  ONLINE    ONLINE    node1
floating_vip  application  ONLINE    ONLINE    node1
...           ...          ...       ...
```

Ein klassisches Startskript in */etc/init.d* für Apache ist von nun an überflüssig, Clusterware startet den Server automatisch beim Neustart des Clusters. Eventuell vorhandene Einträge zum Starten von Apache in */etc/init.d/rc*.d* sollte man entfernen. Ebenso sollte man *apachectl* nicht mehr zum Starten oder Anhalten des Webservers außerhalb von Clusterware verwenden, sondern zu *crs_start apache* et cetera greifen. Sonst vermag Clusterware nicht zu erkennen, dass der Dienst bereits läuft.

Zum Anhalten des Apache dient nun *crs_stop apache*. Mit *crs_relocate* lässt sich eine Ressource manuell vom aktiven auf den passiven Knoten migrieren, was aber normalerweise nicht notwendig ist.

Um den Fehlerfall zu testen, könnte man den aktiven Knoten mit *shutdown -h now* herunterfahren. Auf dem passiven Knoten lässt sich Clusterware daraufhin in Aktion bewundern, am einfachsten mit *watch crs_stat -t*. *watch* ruft *crs_stat -t* alle zwei Sekunden auf. Zuerst zeigt es die Ressourcen von *node1* als „OFFLINE", dann wechseln *floating_vip* und der Apache auf *node2*. (ck)

MARTIN BACH

ist Oracle-Datenbank-Administrator und arbeitet als Consultant mit Schwerpunkt Hochverfügbarkeit und Disaster Recovery in Brighton/England.



Virtualisierte Cold-Standby-Server für Linux

Übernahmebereit

Schlomo Schapiro

Cold-Standby-Server sind eine anerkannte Methode zur Realisierung hochverfügbarer Umgebungen. Will man damit mehrere Produktivserver absichern, steht schnell viel ungenutzte Hardware im Rechenzentrum herum. Mit virtuellen Maschinen und einem SAN lässt sich dieser Overhead deutlich reduzieren.

Eines der erprobten Mittel der Hochverfügbarkeit ist ein „Cold Standby“, ein Reserverechner, der nur bei Ausfall des Hauptservers zum Einsatz kommt. Leider trägt dieser Zweitserver nicht zur Produktivität eines Rechenzentrums bei und ist im flächendeckenden Einsatz zu teuer. Dagegen lässt sich eine virtuelle Maschine (VM) als kostengünstige Alternative (im Idealfall sogar gratis) auch für weniger „wichtige“ Systeme nutzen und kann damit für alle Server im Rechenzentrum einen einfachen Hochverfügbarkeitsschutz bieten.

Virtualisierung ist heute in den meisten Rechenzentren produktiv im Einsatz. Auf den Virtualisierungs-Hosts lassen sich somit ohne weitere Kosten zusätzlich viele Cold Standby VMs betreiben, da sie ja im Regelfall ausgeschaltet sind und keine Ressourcen verbrauchen.

Die Idee, ein Betriebssystem auf unterschiedlichen Plattformen zu betreiben, ist übrigens nicht neu, unter Linux muss man praktischerweise nur einige Treiber austauschen (primär Netzwerk und Festplatte), um dies zu bewerkstelligen. Während man früher gerne auch mal Festplatten eines ausgefallenen Servers in einen neuen umgebaut (oder umgesteckt) hat, kann das heute komfortabel durch den Einsatz einer zentralen Datenablage wie einem SAN (Storage Area Network) geschehen. Damit muss man zum Aktivieren des Cold-Standby-Servers nichts anfassen.

Zunächst ist ein Server ohne lokale Festplatten am SAN zu betreiben, sodass er sein Betriebssystem von dort aus startet. Danach muss man eine virtuelle Maschine so konfigurieren, dass sie dieselbe Logical Unit (LUN) aus dem SAN als primäre Festplatte nutzt. Das Betriebssystem auf dieser SAN-LUN lässt sich nun wahlweise auf der physikalischen Hardware oder auf der virtuellen Maschine starten und verrichtet auf beiden dieselbe Arbeit mit exakt denselben Daten.

Fällt nun die physische Hardware aus, kann der Systemverwalter mit wenigen Mausklicks oder Kommandozeilenbefehlen die virtuelle Maschine starten, und der Server steht wieder zur Verfügung. Dafür muss er keine Festplatte umstecken, keine Daten kopieren oder Dienste umkonfigurieren, der „Cold Standby“ ist sofort nutzbar.

Potenzielle Stolperfallen erkennen

Im Prinzip sind fünf große Klippen zu umschiffen, damit dieses Konzept auch dem harten Alltag und den hohen Anforderungen eines Rechenzentrums gerecht wird. Die erste besteht im Booten aus dem SAN mit mehrpfadiger Anbindung (Multipathing). Die nächste bildet der Start aus dem SAN in der VM ohne Multipathing (diese Funktion deckt die Virtualisierung ab). Das System muss mit den unterschiedlichen Treibern beim Betrieb auf echter Hardware oder in einer VM sowie gegebenenfalls mit leichten Unterschieden in der jeweiligen Konfiguration umgehen können. Letztlich muss man einen gleichzeitigen Systemstart auf Hardware und VM verhindern, da kein gewöhnliches Dateisystem mit einem unkoordinierten Zugriff von zwei Rechnern gleichzeitig zurechtkommt und dies zu einem sofortigen Datenverlust führen würde.

Als Multipathing-Treiber dienen für diesen Artikel die bei Novells Suse Linux Enterprise Server (SLES) 10 standardmäßig integrierten Multipathing-Treiber des Device Mapper und nicht die im HBA-Treiber integrierte Multipathing-Funktion. Das erleichtert später bei der Linux-Konfiguration die Benennung und Zuordnung der einzelnen LUNs.

Anschließend geht es um die Umsetzung mit SLES 10 und einem IBM SAN DS4300 sowie HBAs von Qlogic. Als Hardware fungieren zwei x3650-Rackserver von IBM, einer als „Hardware“ und der andere als Virtualisierungs-Host. Die Anpassungen für

andere Linux-Distributionen und andere SAN-Systeme respektive Hardwaretypen sind trivial, für Windows und andere Betriebssysteme lässt sich das Prinzip, aber nicht die konkrete Umsetzung anwenden.

Als Betriebssystem kommt SLES 10 mit Service Pack 1 und allen aktuellen Updates (mindestens *multipath-tools* und *mkinitrd*) zum Einsatz. Die Virtualisierung realisiert VMwares ESX Server 3.0.2, dessen Funktion „Raw Device Mapping“ die komfortable Einbindung einer SAN-LUN als virtuelle Festplatte erlaubt. Mit anderen Virtualisierungslösungen wie XEN lässt sich aber dasselbe Prinzip ebenso umsetzen.

Installation teils auf Umwegen

In dieser Umgebung ist das Installieren des Betriebssystems etwas komplizierter, da Novell das Einrichten von SLES in das SAN mit Multipathing nicht direkt unterstützt. Weil bei SAN-LUNs ohne Multipathing meist die Schatten-Devices stören (die SCSI-Devices, die nicht funktionieren), ist es einfacher, SLES zunächst in der VM einzuspielen und das aufgespielte System dann für den SAN-Boot anzupassen. In der VM findet sich die SAN-LUN als einfaches Device (*/dev/sda*) ohne Komplikationen.

Bei der Installation sollte man für die Partitionierung und das Formatieren der Dateisysteme „Device-ID“ zum Mounten benutzen, damit in */etc/fstab* gleich die passenden Einträge erscheinen. Die Device-ID ist beim Betrieb in der VM und auf der Hardware identisch, da SLES die ID vom SAN einsetzt, die daher konstant bleibt. Unter ESX gilt das nur für RDM-LUNs (Raw Device Mapping).

Der nächste Schritt besteht im Partitionieren der Systemfestplatte – eine 8 GByte große LUN reicht aus. Sie sollte vier primäre Partitionen */boot* (100 MByte), *swap* (2 GByte), */var* (3 GByte) sowie / (3 GByte) enthalten – formatiert mit Ext3 respektive als Swap.

Für dieses Beispiel ist die Softwareauswahl unerheblich, der Autor empfiehlt als Basis jedoch immer die „Common Code Base“ und das Deselektieren von GNOME beziehungsweise KDE. Damit spielt die Installationsroutine ein relativ schlankes (800 MByte), aber auch vollständiges Basissystem auf. Später lassen sich die tatsächlich benötigten Softwarepakete noch gezielt nachinstallieren, für die Erstellung des Cold Standby ist jedoch schon alles dabei.

Nach der Installation in der VM erfolgt die Anpassung des Systems für den alternierenden Betrieb in der VM und auf der Hardware. Die folgenden Details sind sehr spezifisch für Opensuse ab 10.1 und SLES ab Version 10, bei anderen Distributionen gibt es hier zum Teil größere Abweichungen.

Wechselbetrieb erfordert Anpassungen

Schon in der Initial RAM-Disk (*initrd*) benötigt der Kernel die richtigen Treiber für das Einhängen des Wurzeldateisystems. Auch die Initialisierung des Multipathing muss schon hier erfolgen, da ja das Wurzeldateisystem auch darüber abgesichert sein soll.

Dazu trägt der Administrator die Treiber in */etc/sysconfig/kernel* ein, Listing 1 zeigt ein Beispiel. Entscheidend ist hier die Einbindung der QLogic-Treiber (*qla2xxx*) für die Hardware und der LSI-Logic-Treiber (*mptspi*) für die VM. *dm-rdac* heißt der Multipathing-Treiber für IBMs SAN, bei anderen SAN-Systemen sollte man gegebenenfalls den passenden Multipathing-Treiber benutzen. Damit die USB-Tastatur der Hardware funktioniert, finden sich die USB-HID-Module ebenfalls dort. Der Eintrag der unterschiedlichen Netzwerktreiber (*vmxnet* für VM, *bnx2* und *e1000* für die Hardware) erzwingt eine eindeutige Reihenfolge der Netz-Devices *eth0*, *eth1* et cetera auf beiden Plattformen. Bei 64-Bit-Systemen muss man hier nur den *e1000* für die VM angeben, wenn in der Hardware auch *e1000*-Karten installiert sind. Dies lässt sich Suse-konform auch anders lösen, zum Beispiel durch entsprechende *hwcfg-static-[0,1,2]*-Dateien in */etc/sysconfig/hardware*.

Listing 1: */etc/sysconfig/kernel*

```
INITRD_MODULES="
piix
qla2xxx
mptspi
processor
thermal
fan
jbd
ext3
edd
usbcore
ehci-hcd
ohci-hcd
uhci-hcd
usbhid
vmxnet
bnx2
e1000
dm-rdac"
```

Listing 2: Einstellungen in /etc/*multipath.conf*

```
devices {
      device {
         vendor "IBM"
         product "1814"
         path_grouping_policy "group_by_prio"
         path_checker "rdac"
         hardware_handler "2 rdac 0"
         prio_callout "mpath_prio_tpc /dev/%n"
         failback "immediate"
         no_path_retry "queue"
      }
}
multipaths {
      multipath {
         wwid 3600a0b800029652a0000033746a5b505
         alias system
      }
}
```

In */etc/sysconfig/network/config* schaltet der Eintrag *FORCE_PERSISTENT_NAMES=no* die eindeutige Zuordnung der Netzwerkkarten zu den MAC-Adressen ab. Darüber hinaus sind noch etwaige Einträge in */etc/udev/rules.d/30-net_persistent_names.rules* zu löschen. Damit dieselbe Netzkonfiguration in der VM und auf der Hardware identisch funktioniert, muss man noch die Konfigurationsdateien in */etc/sysconfig/network* gemäß ihrer Interface-Namen *ifcfg-eth0*, *ifcfg-eth1* … umbenennen.

Viele Wege zu einem Ziel

Als Nächstes erfolgt die Anpassung des QLogic-Treibers an das Multipathing des Device Mapper, sodass er SAN-Ausfälle schnell an die darüberliegenden Schichten meldet. Dazu dienen in */etc/modprobe.conf.local* die Moduloptionen *options qla2xxx qlport_down_retry=1 ql2xloginretry_count=5*.

Als Letztes fehlt noch die Konfiguration des Multipathing in */etc/multipath.conf*. Sie enthält zwei wichtige Abschnitte: Der erste (*devices*) definiert die Standardeinstellungen, beispielsweise welche Pathchecker-Methode oder welche Gruppierungs-Policy das System verwenden soll. Dieser muss immer dem verwendeten SAN entsprechen – Listing 2 zeigt die Daten für IBMs DS4300. *multipaths* hingegen definiert die einzelnen LUNs und vergibt auch Aliasnamen für die LUNs, die zur klaren Wiedererkennung wichtig sind. Die ID lässt sich via *multipath -d -v 3* herausfinden und entspricht der Device-ID in */dev/disk/by-id*.

Über den Aufruf *multipath* sollte sich das Multipathing jetzt einfach

iX-TRACT

- Hardwaresysteme lassen sich kostengünstig und mit wenig Aufwand durch eine virtuelle Maschine im Cold-Standby absichern.
- Die Besonderheiten der Konfiguration wie Multipathing und unterschiedliche Treiber bekommt man beim Suse Enterprise Linux mit überschaubarem Aufwand in den Griff.
- Zusammen mit moderner Rechenzentrumstechnik wie SAN und redundanter Anbindung ermöglicht Virtualisierung einen hochverfügbaren Betrieb für mehrere Systeme.

Listing 3: *fstab* mit Multipathing Devices

```
/dev/disk/by-id/scsi-system-part4   /                 ext3     acl,user_xattr           1 1
/dev/disk/by-id/scsi-system-part1   /boot             ext3     acl,user_xattr           1 2
/dev/disk/by-id/scsi-system-part3   /var              ext3     noatime,acl,user_xattr   1 2
/dev/disk/by-id/scsi-system-part2   swap              swap     defaults                 0 0
proc                                /proc             proc     defaults                 0 0
sysfs                               /sys              sysfs    noauto                   0 0
debugfs                             /sys/kernel/debug debugfs  noauto                   0 0
devpts                              /dev/pts          devpts   mode=0620,gid=5          0 0
/var/tmp                            /tmp              none     bind                     0 0
```

Listing 4: GRUB-Konfiguration in */boot/grub/menu.lst*

```
# Modified by YaST2. Last modification on Mon Dec 10 15:58:59 UTC 2007
default 0
timeout 8
###Don't change this comment - YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 10 SP1
    root (hd0,0)
    kernel /vmlinuz-2.6.16.54-0.2.3-smp root=/dev/disk/by-id/scsi-system-part4 vga=normal clock=pmtmr showopts
    initrd /initrd-2.6.16.54-0.2.3-smp
title Rescue in VM
    root (hd0,0)
    kernel /vm/vmlinuz.vm root=/dev/sda4 vga=normal clock=pmtmr init=/bin/bash
    initrd /vm/initrd.vm
###Don't change this comment - YaST2 identifier: Original name: failsafe###
title Failsafe -- SUSE Linux Enterprise Server 10 SP1
    root (hd0,0)
    kernel /vmlinuz-2.6.16.54-0.2.3-smp root=/dev/disk/by-id/scsi-system-part4 vga=normal showopts ide=nodma apm=off acpi=off noresu-
me edd=off 3
    initrd /initrd-2.6.16.54-0.2.3-smp
```

Listing 5: Erstellen der Initial RAM-Disk

```
# mkinitrd -f mpath
Root device:    /dev/disk/by-id/scsi-system-part4 (/dev/dm-13) (mounted on / as ext3)
Module list:    piix mptspi qla2xxx processor thermal fan jbd ext3 edd dm-mod dm-snapshot dm-multipath dm-round-robin
dm-emc dm-rdac dm-hp_sw dm-snapshot-origin dm-striped vmxnet bnx2 e1000 (xennet xenblk dm-mod dm-snapshot)
Kernel image:   /boot/vmlinuz-2.6.16.54-0.2.3-smp
Initrd image:   /boot/initrd-2.6.16.54-0.2.3-smp
Shared libs:    lib64/ld-2.4.so lib64/libacl.so.1.1.0 lib64/libattr.so.1.1.0 lib64/libblkid.so.1.0 lib64/libc-2.4.so
lib64/libcom_err.so.2.1 lib64/libdevmapper.so.1.02 lib64/libdl-2.4.so lib64/libext2fs.so.2.4 lib64/libhistory.so.5.1 lib64/libncur-
ses.so.5.5 lib64/libpthread-2.4.so lib64/libreadline.so.5.1 lib64/librt-2.4.so lib64/libsysfs.so.1.0.3 lib64/libuuid.so.1.2
lib64/libnss_files-2.4.so lib64/libnss_files.so.2 lib64/libgcc_s.so.1
Driver modules: ide-core ide-disk scsi_mod sd_mod piix scsi_transport_spi mptbase mptscsih mptspi scsi_transport_fc
firmware_class qla2xxx processor thermal fan edd dm-mod dm-snapshot dm-multipath dm-round-robin dm-emc dm-rdac dm-hp-sw
libata ahci ata_piix vmxnet bnx2 e1000
Filesystem modules:     jbd ext3
Including:      initramfs dm/mpath fsck.ext3
18136 blocks
```

Listing 6: Ausgabe von *multipath-ll*

```
system (3600a0b800029652a0000033746a5b505) dm-8 IBM,1814      FAStT
[size=1.8T][features=1 queue_if_no_path][hwhandler=2 rdac 0]
\_ round-robin 0 [prio=3][active]
 \_ 0:0:0:0 sda 8:0   [active][ready]
```

Listing 7: Aliasnamen in */dev/disk/by-id*

```
# dir /dev/disk/by-id/scsi-sys*
lrwxrwxrwx 1 root root 10 Feb  1 15:31 /dev/disk/by-id/scsi-system -> ../../dm-8
lrwxrwxrwx 1 root root 11 Feb  1 15:31 /dev/disk/by-id/scsi-system-part1 -> ../../dm-19
lrwxrwxrwx 1 root root 11 Feb  1 15:31 /dev/disk/by-id/scsi-system-part2 -> ../../dm-11
lrwxrwxrwx 1 root root 11 Feb  1 15:31 /dev/disk/by-id/scsi-system-part3 -> ../../dm-20
lrwxrwxrwx 1 root root 11 Feb  1 15:31 /dev/disk/by-id/scsi-system-part4 -> ../../dm-13
```

aktivieren lassen. Leider funktioniert das nicht immer, da ja das laufende System das SCSI-Device schon benutzt. Daher besteht der abschließende Test stets aus einem Systemstart mit einer passenden *initrd*, die Multipathing unterstützt.

Eine Anpassung der */etc/fstab* stellt sicher, dass das System anstelle der Device-ID den Multipathing-Aliasnamen zum Einhängen der Dateisysteme verwendet (s. Listing 3).

Zur Absicherung (falls das System nicht bootet), ist es sinnvoll, die bei der SLES-Installation erstellte *initrd* aufzuheben, weil sich in der VM das System damit immer booten lässt. Da der Suse-*mkinitrd*-Befehl alle Kernel und *initrd*-Images in */boot* abarbeitet, kopiert man den aktuellen Kernel und die aktuelle *initrd* in das zu erstellende Verzeichnis */boot/vm* (*cd /boot*; *mkdir vm*; *cp vmlinuz initrd vm/*) und erweitert die */boot/grub/menu.lst* um einen Eintrag für Rettungs-*initrd* und -kernel. Hier kann man auch gleich bei den regulären Einträgen die Parameter *root=* auf das Multipathing Device ändern (siehe Listing 4).

Beim Booten als „Rescue VM“ muss der Administrator dann */boot* und */var* manuell mounten, da */etc/fstab* ja die Multipathing-Aliasnamen benutzt. Das Rettungssystem startet aber sowieso nur in eine einfache Shell, in der die weiteren Schritte manuell erfolgen. Jetzt kann man via *mkinitrd -f mpath* eine Initial RAM-Disk mit integrierten Multipathing-Treibern generieren lassen, Listing 5 zeigt die Bildschirmausgaben.

Falls sich *mkinitrd* über das fehlende Root-Device beschwert, kann man zum Erstellen auch *mkinitrd -f mpath -d /dev/sda4* nehmen. Die tatsächliche Auswahl des Root Devices erfolgt sowieso durch den Parameter *root=* in der Grub-Konfiguration.

Für den ersten Test startet man das System nochmals in der VM. Das initiiert jetzt schon in der Initial RAM-Disk das Multipathing und hängt das Wurzeldateisystem direkt vom Multipathing Device ein. Eine Kontrolle mit *multipath -ll* sollte eine Ausgabe wie in Listing 6 ergeben. Sie zeigt einen Pfad (in der VM gibt es immer nur einen Pfad), der natürlich auch aktiv ist. In */dev/disk/by-id* finden sich, wie in Listing 7 zu sehen, die zugehörigen symbolischen Links auf die Device Mapper Devices.

Systemstart direkt von der Hardware

Jetzt kann man sich an die Hardware wagen. Dazu muss man zunächst die VM sauber herunterfahren, da sonst die Hardware auf dasselbe Dateisystem zugreifen würde. In der Firmware der HBAs muss man einstellen, dass sie aus dem SAN booten sollen, und dazu die System-LUN als Boot-Device eintragen. Dabei müssen bei jedem HBA die primären Pfade oben in der Liste stehen.

Nach dem obligatorischen Neustart zeigt jetzt ein ohne weitere Konfigurationsanpassungen aus dem SAN bootendes System, dass die Konfiguration in der VM korrekt war. Die korrekte Multipathing-Konfiguration überprüft der Aufruf *multipath -ll*. Klappt das nicht, muss man die Fehlermeldungen genau studieren und wieder in der VM booten und alles richtig einstellen. Besonderes Augenmerk gilt hier der Netzkonfiguration, die auf der Hardware und in der VM identisch funktionieren sollte. Falls in der Hardware mehrere Netzwerkkarten installiert sind, kann es erforderlich sein, auch in der VM mehrere zu installieren. Auch wenn davon nicht alle mit einem Netz verbunden sind, lassen sich dadurch unschöne Verschiebungen vermeiden. Nach jeder Anpassung an der Systemkonfiguration sollte man die Dual-Boot-Fähigkeit nochmals prüfen, um die Ausfallsicherheit nicht zu gefährden.

Darüber hinaus sollten technische Mittel sicherstellen, dass Hardware und VM nicht zeitgleich arbeiten. Hier bietet sich beispielsweise ein Patch der Initial RAM-Disk an, der mit einem einfachen Ping-Test den gleichzeitigen Betrieb verhindert. Leider darf man dann kein *mkinitrd*-Update mehr installieren, weshalb der Autor bei SLES 10 SP 1 den manuellen Weg empfiehlt. Falls das Standby-System (in der Regel die VM) immer eingeschaltet ist, aber in der Initial RAM-Disk vor dem Einhängen des Wurzeldateisystems verbleiben würde, bis das Hauptsystem für eine Weile ausgefallen ist, hätte man damit schon eine automatische Übernahme bei Komplettausfall der Hardware umgesetzt.

Opensuse verfügt seit Version 10.3 über eine verbesserte Initial RAM-Disk, bei der sich eigene Skripte leicht in den *mkinitrd*-Prozess integrieren lassen. Bei SLES 10 ist hierzu noch ein direkter Patch des */sbin/mkinitrd*-Skripts nötig. Beim kommenden SLES 11 dürfte sich somit dann auch die Automatik und Überwachung herstellerkonform integrieren lassen.

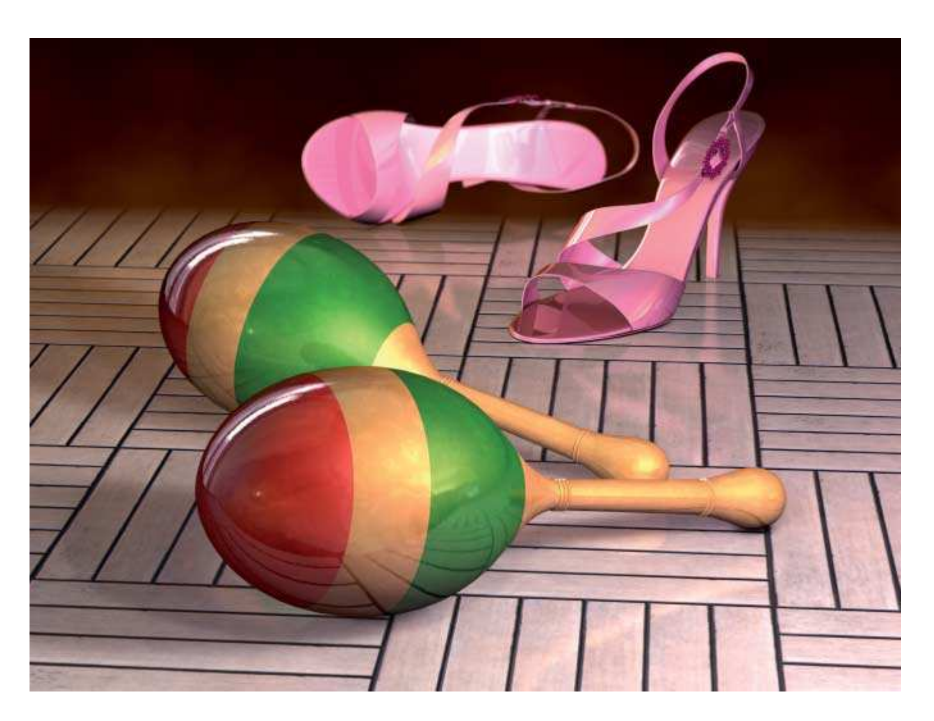
Fazit

Mit dem vorgestellten Vorgehen zur Absicherung physikalischer Server durch virtuelle Maschinen lassen sich Kosten senken und man kann die Virtualisierung auch für solche Systeme gewinnbringend nutzen, die sonst keine Virtualisierungskandidaten sind. Bei einem Ausfall der Hardware wird man immer eine geringere Leistung oder eine fehlende Herstellerzertifizierung hinnehmen können, wenn dafür die „Kundschaft“ wie gehabt weiter arbeiten kann.

Hier kommen die Möglichkeiten der modernen Rechenzentrumstechnik wie Multipathing, SAN-Boot und zentrale Datenablage sowie die Virtualisierung in einer einfachen, aber wirkungsvollen Gesamtlösung zusammen. Mit vergleichbar geringen Kosten lässt sich kein anderes Hochverfügbarkeitsszenario aufbauen, die hier erreichbaren Umschaltzeiten von fünf Minuten (mit Automatik) bis einer Stunde (manuell, inklusive Wecken des Admins und VPN-Einwahl) dürften für die meisten Anwendungen mehr als hinnehmbar sein. (avr)

SCHLOMO SCHAPIRO

ist Senior Consultant und leitet den Bereich Open Source & Virtualisierung bei der probusiness Group.



Linux-Server als Domänenmitglied

Rhythmuswechsel

Volker Lendecke

In gemischten Umgebungen bereiten die unterschiedlichen Ansätze zur Benutzerverwaltung oft Schwierigkeiten. Samba lässt sich als Mitgliedsserver einer Windows-Domäne flexibel konfigurieren und hilft, manche Klippe zu umschiffen.

Im ersten Teil des Tutorials stand der Einsatz von Samba als Standalone-Server im Mittelpunkt. Wesentlich daran ist, dass Samba die Benutzer und Passwörter selbst kennt und verwaltet. In den meisten Firmen existiert heute jedoch schon eine zentrale Benutzerverwaltung, entweder noch in Form einer NT4-kompatiblen Domäne oder eines Active Directory. Samba ist selbstverständlich in der Lage, die dort verwalteten Benutzer und Gruppen zu verwenden. Wie das funktioniert, beschreibt dieser zweite Teil.

Wesentlich für die Authentifizierung von Benutzern ist der Parameter *security*, der fünf Einstellungen kennt:

[share] ist veraltet und sollte nicht mehr zum Einsatz kommen. Mit dieser Einstellung lassen sich einzelne Benutzer nicht unterscheiden, jede Freigabe bekommt ein Passwort.

[user] ist die Standardeinstellung, mit der Samba Benutzer und Passwörter selbst verwaltet. Dies gilt für Standalone-Server ebenso wie für Domänencontroller (DC), die im dritten Teil des Tutorials Thema sein werden.

[server] ist ebenfalls veraltet und man sollte darauf verzichten. Wurde durch *security=domain* ersetzt.

[domain] bewegt Samba dazu, mit NT-konformen Mitteln die Authentifizierung an einen DC zu delegieren. Aus Sicht des Samba-Clients ist dies gleichwertig mit *security=user*, der Unterschied liegt ausschließlich darin, wie Samba die Passwörter überprüft.

[ads] ist in vielerlei Hinsicht äquivalent zu *security=domain*, nur dass Samba dem Client zusätzlich Kerberos als Authentifizierungsmethode anbietet.

Damit Samba die Benutzerauthentifizierung einer Domäne verwenden kann, muss der Server als Erstes die Domäne betreten. Mit diesem Schritt erstellt der Administrator ein Maschinenkonto in der Domäne mit einem zufällig gewählten Passwort für dieses Konto. Existiert schon ein Konto für die Maschine, so wird nur das Passwort auf einen neuen, zufälligen Wert gesetzt.

Beitritt zu einer Windows-Domäne

Das Maschinenkonto ist eine Voraussetzung, um zwischen dem Mitgliedsserver und der Domäne eine Vertrauensstellung herzustellen. Diese ist nicht so sehr notwendig, damit der DC feststellen kann, dass der Samba-Server Berechtigungen in der Domäne hat, sondern die umgekehrte Authentifizierung ist wichtig: Der Samba-Server muss sich überzeugen können, dass der DC – der letztlich die Passwortüberprüfung durchführt – wirklich vertrauenswürdig ist. Ohne diese Überprüfung stünden Windows-Domänen vor dem gleichen Problem wie NIS oder ein nicht sicher eingerichtetes *nss ldap*/*pam ldap*: Jeder, der die IP-Adresse des Servers mit der Benutzerdatenbank fälscht, kann sämtliche Mitgliedsrechner übernehmen.

Zum Betreten einer Domäne muss man in der *smb.conf* bei *workgroup* den Domänennamen angegeben und den Parameter *security = domain* setzen:

```
[global]
workgroup = w2k3ad
security = domain
```

Jetzt kann der Administrator den Befehl *net rpc join* absetzen:

```
server:/root # net rpc join -U Administrator
Enter Administrator's password:
Joined domain W2K3AD.
server:/home/vlendec #
```

Mit diesem Schritt erzeugt der *net*-Aufruf das Maschinenkonto in der Domäne. Er hat zudem das Passwort auf einen zufälligen Wert gesetzt. Der Name des Maschinenkontos ist der Wert des Parameters *netbios name*, der standardmäßig mit dem Hostnamen der Maschine vorbelegt ist. Mit den obigen Einstellungen erzeugt der Aufruf also das Maschinenkonto unter dem Namen *server*.

net rpc join speichert das Maschinenpasswort des Servers in der Datei *secrets.tdb*, die typischerweise in */etc/samba/* liegt. Via *tdbdump secrets.tdb* kann man es sich ansehen. Geht die Datei *secrets.tdb* aus irgendwelchen Gründen verloren, ist die Domänenmitglied-

schaft des Samba-Servers zerstört, ein erneutes *net rpc join* erstellt sie neu.

Im Beispiel diente zum Betreten der Benutzer „Administrator“. Es ist klar, dass spezielle Privilegien in der Domäne zum Betreten notwendig sind, der Vorgang legt ja ein neues Benutzerkonto an. Windows kann dieses Recht an Nicht-Administratoren delegieren, Samba genügt zum Betreten der Domäne ein entsprechend privilegierter Account.

Wenn Samba der Domäne erfolgreich beigetreten ist, muss man den *smbd* neu starten. Verbindet sich jetzt ein Benutzer, fragt der *smbd* bei einem DC nach, ob das Passwort richtig ist.

Der nächste Fall: Active Directory

Benutzt man den Modus *security=domain*, verbindet sich Samba mit NT4-kompatiblen Methoden mit den Domänencontrollern. Dies ist zur Authentifizierung das NTLM-Verfahren (NT LAN-Manager) in seinen unterschiedlichen Ausprägungen bis hin zu NTLMv2, das Samba auch unterstützt, die Benutzerverwaltung erfolgt über sogenannte RPC-Methoden. Mit Windows 2000 hat Microsoft Active Directory eingeführt, das zur Authentifizierung bevorzugt Kerberos einsetzt und zur Benutzerverwaltung ein LDAP-Verzeichnis anbietet. Die Frage, ob man Samba besser im Modus *security=domain* oder *security=ads* betreiben soll, lässt sich nicht einfach beantworten. Als Entscheidungshilfe folgen ein paar Argumente für und gegen *security=ads*.

Jedes Active Directory kann Samba-Server im Modus *security=domain* als Mitglied aufnehmen. Es ist ein häufig anzutreffendes Missverständnis, dass dies nur für Domänen im sogenannten „Mixed Mode“ gilt. Selbst Domänen im Windows-2003-Infrastruktur-Modus sind in der Lage, NT-kompatible Mitglieder aufzunehmen. Das einzige, was nur Mixed-Mode-Domänen tun, ist die Aufnahme von NT4-Backup-Domänencontrollern (BDC). Da Samba aber ohnehin kein solcher BDC werden kann, ist dieser Aspekt irrelevant.

Politische Gründe in der Firma können die Benutzung von Kerberos erfordern. Es gilt allgemein als deutlich sicherer als NTLM, wobei NTLMv2 ebenfalls durchaus einen vernünftigen Sicherheitsstandard vorzuweisen hat.

Ein Vorteil von Kerberos gegenüber der NT-Authentifizierung ist die reduzierte Anmeldelast auf den Domänencontrollern. Mit den NT-Methoden muss ein Mitgliedsserver bei jeder Benutzeranmeldung beim Domänencontroller nachfragen, ein Kerberos-Ticket ist einerseits für eine gewisse Zeit gültig und steht für sich alleine. Legt ein Anwender ein gültiges Ticket vor, genügt das dem Samba-Server, er muss nicht mehr beim DC nachfragen.

Windows 2003 hat einen Bug beim Auflisten mit den NT-kompatiblen RPC-Methoden: Es zeigt nur die ersten 100 Benutzer an. Listet man sie via LDAP auf, bekommt man alle. Das Auflisten von Benutzern ist eine Operation, die man vermeiden sollte, denn bei großen Domänen kann dieser Vorgang extrem lange dauern. Unter Umständen ist der 100-User-Bug auch gar kein Fehler, sondern Absicht. Ist man jedoch auf das Auflisten der Benutzer angewiesen, muss man *security=ads* wählen.

Im Active Directory existiert das Konzept der sogenannten Standorte oder Sites. Jeder Domänencontroller und Mitgliedsrechner ist einem Standort zugeordnet. Will sich ein Mitgliedsrechner mit einem Domänencontroller verbinden, dann sollte dies nur innerhalb eines Standortes geschehen. Die entsprechenden Mechanismen benutzt Samba nur im Modus *security=ads*.

security=ads ist sehr kritisch bezüglich koordinierter Serverzeit und korrekt funktionierendem DNS. Wenn Samba einen Domänencontroller sucht, geschieht dies bei *security=ads* via DNS, die Authentifizierung geschieht per Kerberos. Die Sicherheit von Kerberos beruht zum Teil darauf, dass sich alle Rechner im Netz über die Uhrzeit einig sind. Ist dies nicht der Fall, verweigert es den Zugang. Das heißt, wer *security=ads* einsetzen möchte, ist gut beraten, in */etc/resolv.conf* einen Windows-DNS-Server als Nameserver und den gleichen Server in */etc/ntp.conf* als Zeitserver einzutragen. Ebenso muss die Datei */etc/krb5.conf* korrekt konfiguriert sein, damit die Authentifizierung auch klappt, Listing 1 zeigt ein Beispiel.

Listing 1: */etc/krb5.conf* (1)

```
[libdefaults]
        default_realm = W2K3AD.ORG

[realms]
        W2K3AD.ORG = {
                kdc = 192.168.234.18
        }

[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON
```

Älteren Kerberos-Bibliotheken bereiten die im AD verwendeten Krypto-Algorithmen häufig massive Schwierigkeiten. Entweder unterstützen sie das benötigte HMAC-MD5 gar nicht, oder die Implementierungen sind mangels Benutzung fehlerhaft. Viele (leider nicht alle …) als Samba-Bug gemeldete Crashs sind in Wahrheit durch Kerberos verursachte Abstürze. Moderne Linux-Distributionen haben diese Stolperfallen nicht mehr, aber insbesondere Hersteller proprietärer Unixe liefern ihre Betriebssysteme teilweise noch mit zu alten Kerberos-Bibliotheken aus.

Als Quintessenz kann man sagen, dass *security=ads* vielfach wünschenswert, aber viel komplizierter als *security=domain* sein kann. Insbesondere in kleinen Domänen mit nur einem Standort beziehungsweise LAN reicht *security=domain* häufig völlig aus.

Beitritt zu einem Active Directory

Für *security=ads* sieht die *smb.conf* leicht verändert aus:

```
[global]
workgroup = W2K3AD
realm = W2K3AD.ORG
security = ads
```

Gegenüber *security=domain* kommt der Parameter *realm* hinzu, der dem voll qualifizierten Langnamen der Domäne in Großbuchstaben entsprechen muss. Kerberos unter Unix unterscheidet Groß- und Kleinbuchstaben, sodass ein in Kleinbuchstaben geschriebener Parameter *realm* zu recht merkwürdigen Fehlermeldungen führen kann. */etc/krb5.conf* könnte im Beispiel wie in Listing 2 aussehen. Mit dem Aufruf *net ads join* betritt ein Server die Domäne, Listing 3 zeigt die Bildschirmausgabe.

Sollte dieser Vorgang fehlschlagen, kann das aus verschiedenen Gründen geschehen. Der sicherste Weg zur Fehlersuche ist ein sauberes DNS- und Zeit-Setup. Der FQDN des Samba-Servers muss sich korrekt innerhalb der

iX-TRACT

- Samba kann über den Parameter „security=…“ die Passwortüberprüfung an externe Systeme delegieren.
- In Windows-Umgebungen lassen sich für die Authentifizierung NT-Domänen oder ein Active Directory verwenden.
- Winbind bindet die Kerberos-gesicherte AD-Benutzerverwaltung in Unix-Systeme ein.

Listing 2: */etc/krb5.conf* (2)

```
[libdefaults]
     default_realm = W2K3AD.ORG

[realms]
     W2K3AD.ORG = {
          kdc = 192.168.234.18
          admin_server = 192.168.234.18
     }
```

Listing 3: Ausgabe von *net ads join*

```
server:/home/vlendec # net ads join -UAdministrator
Using short domain name -- W2K3AD
Joined 'SERVER' to realm 'W2K3AD.ORG'
server:/home/vlendec #
```

Listing 4: Ausgaben von *wbinfo*

```
delphin:~ # wbinfo -t
checking the trust secret via RPC calls succeeded

delphin:~ # wbinfo -a windows\\vl%asdf
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

Windows-Domäne befinden, die *krb5.conf* korrekt konfiguriert sein und die Zeit stimmen.

Winbind – ein zentraler DC-Verbindungsproxy

Mit dem Betreten der Domäne ist der *smbd* in der Lage, Benutzer beim Domänencontroller zu authentifizieren. Je nach Security-Modus und der Auswahl des Clients geschieht dies durch Auswertung des Kerberos-Tickets oder durch Nachfragen beim DC. Insbesondere Letzteres ist aufwendig, da der *smbd* sich einen Domänencontroller suchen und dann mit dem Maschinenkonto anmelden muss, bevor er die Benutzerauthentifizierung durchführen kann. Dies generiert mindestens 30 Netzpakete, von denen nur zwei die eigentliche Authentifizierung realisieren.

Windows arbeitet hier anders: Die Local Security Authority (LSA) baut beim Start des Domänenmitglieds einmal eine Verbindung zum DC auf und authentifiziert sich als Maschine. Benutzerauthentifizierungen laufen danach nur noch über diese Verbindung. Via *smbd* allein funktioniert dies nicht, da es für jeden Client einen eigenen Prozess gibt und sich Netzwerkverbindungen nicht einfach von mehreren Prozessen gleichzeitig nutzen lassen.

Als Proxy für die Verbindung zum DC entwarfen die Samba-Entwickler den *winbindd*. Er übernimmt mehr und mehr die Rolle der LSA unter Windows, insbesondere hält er eine Verbindung zum DC offen und bietet seine Dienste für alle Prozesse im System hinter einem Unix Domain Socket unter */tmp/winbindd/pipe* an. Der *smbd* versucht bei einer Authentifizierung zunächst, sich mit dem Socket zu verbinden. Erst wenn dies fehlschlägt, initiiert er selbst eine direkte Verbindung mit einem DC. Den *winbindd* muss man einfach nur starten, um seine Dienste nutzen zu können.

Als Testprogramm für *winbindd* gibt es das Programm *wbinfo*. Wenn der *winbindd* gestartet ist, kann man ihm mit *wbinfo -p* ein Ping schicken. Den Test, ob *winbindd* sich korrekt mit dem Domänencontroller verbinden konnte, erledigt *wbinfo -t*, eine Authentifizierungsanfrage kann man mit *wbinfo -a* auslösen. Die dazugehörigen Bildschirmausgaben zeigt Listing 4.

nsswitch: Namensauflösung von Benutzern

Dass ein Benutzer authentifiziert ist, reicht noch lange nicht aus, um auf das System zuzugreifen. Samba braucht grundsätzlich für jeden Client-Benutzer ein Unix-Gegenstück, damit es die Zugriffskontrolle im Dateisystem dem Kernel überlassen kann. Das heißt, dass jeder Domänenbenutzer mit allen seinen Gruppenmitgliedschaften in Unix existieren muss. Auf einem Heimserver mag das noch realistisch sein, aber in größeren Domänen fällt die Möglichkeit, alle Benutzer unter Unix nachzupflegen, schlicht aus.

Analog zu *nss_ldap* stellt Samba das Modul *nss_winbind* zur Verfügung, mit dem es Benutzer und Gruppen dynamisch vom Domänencontroller beziehen kann. Zum Aktivieren dieses Moduls sind in */etc/nsswitch.conf* die Einträge für *passwd* und *group* anzupassen:

```
passwd: files winbind
group: files winbind
```

Mit diesen Einstellungen sucht das Betriebssystem Benutzernamen erst in */etc/passwd*. Findet sich ein Benutzer dort nicht, kontaktiert es den *winbindd*.

Damit Letzterer in der Lage ist, aus einem Benutzernamen einen vollständigen *passwd*-Eintrag zu erzeugen, muss er zwei Schritte durchführen. Als Erstes erfragt er bei Windows den dortigen Benutzernamen und generiert daraus einen sogenannten Security Identifier (SID). Im zweiten Schritt wird der SID zu einer Unix-UID. Gleiches geschieht mit der primären Gruppe des Benutzers. Winbind vollzieht beide Schritte automatisch nacheinander, sie können aber unabhängig voneinander fehlschlagen. Die Auflösung eines Namens zu einem SID erfolgt per *wbinfo -n*:

```
delphin:~ # wbinfo -n windows\\administrator
S-1-5-21-72162050-2052214257-1551924553-↙
                                        500 User (1)
```

ID Mapping – Umsetzung zwischen den Welten

Einen Namen zu einem SID zu übersetzen ist einfach, denn das erledigt der DC für Samba. Viel schwieriger ist es, für diesen SID eine Unix-Identität zu finden. Der DC weiß normalerweise nichts von Unix-IDs, das heißt, Winbind muss sich die Unix-IDs quasi selbst ausdenken. Die einfachste Konfiguration hierfür besteht einfach nur aus den Einstellungen

```
uid range = 1000000-2000000
gid range = 1000000-2000000
```

Mit diesen Parametern im Abschnitt *[global]* der *smb.conf* sichert der Systemverwalter *winbindd* zu, die genannten Bereiche nicht in der lokalen Benutzerdatenbank zu verwenden. Meldet sich ein unbekannter Benutzer an, alloziert *winbindd* eine neue UID aus dem gegebenen Bereich, und speichert die Zuordnung in der *winbindd_idmap.tdb*. Die Zuordnungen vergibt *winbindd* dabei fortlaufend.

Bezüglich des Backups hat die Datei *winbindd_idmap.tdb* den Status der */etc/passwd*. Ein Verlust der Datei führt zum Verlust sämtlicher Rechtezuordnungen im Dateisystem. Es ist nicht mehr festzustellen, wer Benutzer „1004711“ wirklich ist. Daher sollte man von der *winbindd_idmap* regelmäßig Datensicherungen durchführen. Dies ist als direkte Kopie schwierig, da es sich um eine Binärdatenbank handelt, die Winbind im laufenden Betrieb offen hält. Ein Backup lässt sich auf zwei verschiedene Arten durchführen: Entweder liefert das Kommando *tdbbackup* eine *tdb*-Datei, die im Wiederherstellungsfall die existierende *winbindd_idmap.tdb* ersetzen kann, oder der Aufruf *net idmap dump* führt zu einer Klartextdatei, die sich per *net idmap restore* wieder einspielen lässt.

Tutorialinhalt

Solange nur ein Server in Betrieb ist, funktioniert die fortlaufende Zuordnung in einer *tdb*-Datei gut. Mit mehr als einem Server treten Schwierigkeiten auf, da sich Benutzer nicht gleichartig zuordnen lassen. Beispielsweise bekommt der User Meier auf einem Server die UID 1004711, auf einem anderen Server die uid 10000815 zugeordnet. Spätestens mit NFS-Mounts führt dies zu Chaos.

Es existieren mehrere Möglichkeiten, dieses zu umgehen. Neben der fortlaufenden Nummerierung kann Winbind Unix-IDs flexibel zuweisen. Bis zur Samba-Version 3.0.25 war der einzig unterstützte Weg, die *idmap* über Rechnergrenzen hinweg zu koordinieren, ein LDAP-Server. Mit

```
idmap backend = ldap:ldap://servername/
ldap suffix = dc=samba,dc=org
ldap admin dn = cn=sambaadmin,dc=samba,dc=org
```

kann Winbind die allozierten Unix-IDs in einer LDAP-Datenbank speichern. Wie bei der Konfiguration des Backends *ldapsam passdb* muss man auch hier mit *smbpasswd -w* das Passwort des LDAP-Admin *dn* angeben.

Warum ist es überhaupt so kompliziert, sich Unix-IDs aus den Fingern zu saugen? Auch Windows weist jedem Benutzer und jeder Gruppe eine eindeutige ID zu, den SID. Der enthält einen Domänenanteil aus 96 Bit, und einen innerhalb der Domäne eindeutigen Relative Identifier (RID). Warum nimmt man nicht einfach diesen als Unix-ID? Solange man nur eine Domäne hat, klappt das reibungslos. Schwierig wird dies bei Vertrauensstellungen. Vertraut die Domäne, in der Samba Mitglied ist, einer anderen Domäne, ist der RID nicht mehr eindeutig. Die 500 bezeichnet grundsätzlich den Administrator, 513 ist immer den Domänenbenutzern zugeordnet, und ab 1000 aufwärts vergibt jede Domäne fortlaufend RIDs.

Vor der Version 3.0.25 konnte man mit *idmap backend = rid* für die Ein-Domänen-Umgebung die RIDs als Unix-IDs verwenden und so ebenfalls Chaos mit mehreren Servern vermeiden. Sobald jedoch die Hauptdomäne, in der Samba Mitglied ist, einer anderen Domäne vertraut, funktioniert das aus den oben angesprochenen Gründen nicht mehr. Daher haben die Entwickler mit der 3.0.25 das *idmap*-Subsystem (wieder einmal) umgeschrieben.

Der wesentliche neu eingeführte Parameter heißt *idmap domains*. Er gibt an, für welche Domänen Samba eine Sonderkonfiguration vornehmen soll. Wie das funktioniert, beschreibt am besten ein Beispiel (siehe Listing 5). Es konfiguriert für die beiden Domänen *WINDOWS* und *TRUSTED* jeweils einen Bereich von 99 999 Unix-IDs, den diese verwenden können. Die Unix-ID berechnet sich dabei aus dem RID zuzüglich der unteren Grenze des ID-Bereichs. *TRUSTED\Administrator* würde so beispielsweise die UID *200500* zugewiesen bekommen. Weitere *idmap*-Backends führt der Kasten „Backends für ID-Mapping“ kurz auf. Jedes dieser Backends hat individuelle Konfigurationsparameter, die man den Manpages (*man idmap_[backendname]*) entnehmen kann.

Listing 5: Neuer Parameter *idmap* im Einsatz

```
idmap domains = WINDOWS TRUSTED
idmap config WINDOWS:backend  = rid
idmap config WINDOWS:range    = 100000 - 199999
idmap config TRUSTED:backend  = rid
idmap config TRUSTED:range    = 200000 - 299999
```

Listing 6: Erweiterte Benutzerinfos via SFU

```
idmap config WINDOWS:backend  = ad
idmap config WINDOWS:schema_mode = sfu
idmap config WINDOWS:range    = 100000 - 199999
winbind nss info = sfu
```

Backends für ID-Mapping

[tdb] ist die Default-Einstellung. Winbind erstellt die ID-Mappings selbstständig und speichert sie lokal in einer *tdb*-Datei. Dies ist sinnvoll, wenn man nur einen einzigen Mitgliedsserver benutzt oder die Unix-IDs nicht serverübergreifend synchron halten muss.

[rid] verwendet den Relative Identifier, die letzte Komponente des Windows-SID, direkt als Unix-ID. Zum Realisieren von Vertrauensstellungen lassen sich pro Domäne Offsets angeben. Das RID-Backend lässt sich gut benutzen, wenn nur eine kleine Anzahl von Domänen vorhanden ist.

[ad] lässt sich verwenden, wenn im Active Directory die Erweiterungen für die Services For Unix (SFU) implementiert sind. Im Rahmen dieser Extensions kann der Administrator explizit Unix-IDs vergeben. Diese liest der Winbind aus.

[ldap] speichert die selbst gewählten ID-Mappings in einem LDAP-Verzeichnis und ermöglicht so die Koordination unterschiedlicher ID-Mappings.

[nss] nimmt gar kein Mapping anhand von SIDs vor, sondern setzt voraus, dass Domänencontroller und -mitglied die */etc/passwd* mit anderen Mitteln, etwa per *nss_ldap*, synchronisieren. Fragt ein System den Winbind dennoch nach einem Mapping, liefert er dies namensbasiert. Das heißt, er konvertiert einen SID zunächst in den zugehörigen Namen und schaut dann in */etc/passwd* nach.

Shell, Heimatverzeichnis et cetera

Neben der User-ID muss Winbind die Login-Shell und das Heimatverzeichnis eines Benutzers festlegen. Beides kennt ein typischer Windows-Domänencontroller nicht. Standardmäßig steuern die Parameter *template homedir* und *template shell* die beiden Werte. Dies ist der einzige Weg, Benutzerinformationen auf NT4-Domänenmitgliedern zu vervollständigen. Kommt das *idmap_ad backend* für das UID-Mapping zum Einsatz, kann Winbind das Heimatverzeichnis aus eventuell vorhandenen SFU-Informationen (Services for Unix) beziehen. Dazu muss man den Parameter *winbind nss info* auf einen der Werte *rfc2307*, *sfu* oder *sfu20* setzen, je nach verwendeter SFU-Version.

In der Beispielkonfiguration in Listing 6 setzen die Einstellungen voraus, dass auf dem Domänencontroller die Services for Unix installiert und die Unix-Attribute der Benutzer gepflegt sind. Die */etc/passwd*-Einstellungen für die Benutzer übernimmt der Samba-Server damit komplett aus dem AD.

Mit der Anbindung an die Firmen-Infrastruktur durch Winbind ist ein Samba-Fileserver im Administrationsaufwand nicht mehr von einem Windows-Fileserver zu unterscheiden. Die komplette Benutzerverwaltung von Passwörtern angefangen über Gruppenzuordnungen bis hin zu Unix-Attributen kann das Active Directory übernehmen. In diesem Tutorial nicht dargestellt sind die Offline-Fähigkeiten des Winbind. Damit lassen sich nicht nur Fileserver, sondern auch Arbeitsplatzrechner und Laptops analog zu Windows-Clients in ein AD einbinden. Der mit nach Hause genommene Laptop funktioniert genau so, wie es der Anwender von seinem Windows-Client erwartet. (avr)

VOLKER LENDECKE

ist Mitglied des Samba-Teams und Mitbegründer der Service Network GmbH in Göttingen.

Bloomfilter: Schnelle, ungenaue Suche

Planten un Bloomen

Michael Riepe

Einen guten Teil ihrer Zeit verbringen Computer mit dem Suchen in Listen, Bäumen oder Feldern. Mitunter lässt sich der Aufwand jedoch erheblich reduzieren.

Wer sucht, der findet – sagt man. Leider trifft die Aussage in der IT-Welt eher selten zu. Vor allem, weil eine erfolglose Suche oft länger dauert als eine erfolgreiche. Um etwa festzustellen, ob sich ein bestimmter Schlüssel in einer unsortierten Liste befindet, muss ein Programm die gesamte Liste durchlaufen. Eine positive Antwort hingegen erhält es im Schnitt nach der Hälfte der Schritte.

In Bäumen oder sortierten Feldern lassen sich Daten schneller finden: Die Suchzeit wächst in der Regel logarithmisch mit der Zahl der gespeicherten Datensätze (*O(log n)*). Noch schneller sind Hashtabellen: Solange keine Kollisionen auftreten, bleibt die Suchzeit konstant. Andernfalls wächst sie je nach Implementierung linear oder logarithmisch.

Erheblichen Einfluss hat das verwendete Speichermedium. Auf der Festplatte etwa dauert eine Suche um Größenordnungen länger als im Hauptspeicher. Ein Index im RAM kann Abhilfe schaffen oder die Auswirkungen zumindest lindern – sofern der Platz dafür ausreicht.

Ja, nein und vielleicht

1970 entwickelte Burton H. Bloom für ein Rechtschreibprüfprogramm eine besonders kompakte Darstellung: den Bloomfilter. Statt eine Wortliste in seine Software einzubinden, berechnete er mehrere Hashwerte aller Wörter und notierte sie in einem Bitfeld (siehe Listing 1). Will man im Bloomfilter einen bestimmten Schlüssel finden, muss man dessen Hashwerte berechnen und die dazugehörigen Bits untersuchen. Hat eins den Wert *0*, ist der Datensatz garantiert nicht vorhanden. Sind alle gesetzt, besteht eine gewisse Wahrscheinlichkeit, dass er gespeichert ist.

Darin besteht einer der Nachteile des Bloomfilters: Er gibt nicht immer eine exakte Antwort, sondern beschränkt sich auf „nein“ und „vielleicht“. Die Wahrscheinlichkeit *P*, dass das Vielleicht sich als Nein entpuppt (False Positive), hängt vom Füllgrad – dem Prozentsatz gesetzter Bits – und der Zahl der verwendeten Hashfunktionen ab:

$$P = \text{Füllgrad}^{\text{Zahl der Hashes}}$$

Ist zum Beispiel das Bitfeld zu 10 % gefüllt und kommen drei Hashfunktionen zum Einsatz, erweist sich von 1000 positiven Antworten durchschnittlich eine als falsch. Bei einem zur Hälfte gefüllten Bitfeld bedeutet jedoch bereits jedes achte Vielleicht tatsächlich Nein. Es empfiehlt sich daher, den Füllgrad niedrig zu halten. Formeln für die Berechnung sind unter anderem im englischen Wikipedia-Eintrag zu finden (siehe Kasten „Onlinequellen“). Wer mit Mathematik auf dem Kriegsfuß steht, kann sich die Parameter auch online ausrechnen lassen.

Ein weiterer Nachteil des klassischen Bloomfilters ist, dass sich Einträge nicht entfernen lassen. Nach dem Löschen von Datensätzen muss das Programm den Inhalt des Bitfelds neu berechnen. Alternativ kann es mitzählen, wie oft es ein bestimmtes Bit gesetzt hat. Fällt beim Entfernen der Zähler auf Null, muss es das Bit wieder löschen. Allerdings beanspruchen die Zähler erheblich mehr Speicherplatz als das Bitfeld. Kommen Einfüge- und Löschoperationen relativ selten vor, kann man die Zähler jedoch auf den Massenspeicher auslagern, ohne dass die Performance stark darunter leidet – beim Suchen benötigt man sie nicht.

Bloomfilter im Einsatz

In begrenztem Umfang unterstützen Bloomfilter auch die übrigen für Mengen (Sets) definierten Operationen. Vereinigungs- und Schnittmenge erhält man durch bitweise Oder- beziehungsweise Und-Verknüpfung der Bitfelder. Die müssen dazu natürlich gleich groß sein; außerdem müssen die Filter dieselben Hashfunktionen verwenden. Die Subtraktion zweier Mengen lässt sich leider nicht mit einfachen Bit-Operationen realisieren. In manchen Fällen hilft ein zweiter Bloomfilter, der die entfernten Elemente aufnimmt. Allerdings kann es vorkommen, dass beide Filter behaupten, ein bestimmtes Element zu enthalten. Welcher die Wahrheit sagt, lässt sich nur durch eine Analyse der Daten feststellen. (mr)

Listing 1: Bloomfilter in C

```c
#define ANZAHL_BYTES    65536u
#define ANZAHL_BITS     (ANZAHL_BYTES / 8u)
unsigned char bitfeld[ANZAHL_BYTES];
void set_bit(unsigned x) {
    bitfeld[x / 8] |= 1u << x % 8;
}
int test_bit(unsigned x) {
    return bitfeld[x / 8] & (1u << x % 8);
}
void wort_hinzufuegen(const char *wort) {
    unsigned h;
    h = hash_1(wort) % ANZAHL_BITS; set_bit(h);
    h = hash_2(wort) % ANZAHL_BITS; set_bit(h);
    ...
    h = hash_k(wort) % ANZAHL_BITS; set_bit(h);
}
int wort_vorhanden(const char *wort) {
    unsigned h;
    h = hash_1(wort) % ANZAHL_BITS; if (!test_bit(h)) return 0;
    h = hash_2(wort) % ANZAHL_BITS; if (!test_bit(h)) return 0;
    ...
    h = hash_k(wort) % ANZAHL_BITS; if (!test_bit(h)) return 0;
    return 1;
}
```

Ein Bloomfilter lässt sich mit wenigen Zeilen Code realisieren. Allerdings fehlen noch die Hashfunktionen.

Onlinequellen

Wikipedia (deutsch)
de.wikipedia.org/wiki/Bloomfilter

Wikipedia (englisch)
en.wikipedia.org/wiki/Bloom_filter

Dimensionierungsrechner
www.cc.gatech.edu/fac/Pete.Manolios/bloom-filters/calculator.html

Allergien gegen alles und jeden

Gesundheit!

Diane Sieger

Lang, lang ist's her, dass der Heuschnupfen die einzige allgemein bekannte Allergie war. Mittlerweile weiß man von allergieauslösenden Stoffe in allen Facetten – und jeder kennt sicherlich mindestens einen Allergiker, wenn er nicht sogar selbst betroffen ist.

Jeder dritte Erwachsene in Deutschland leidet an einer Allergie. Der Kontakt mit einem bestimmten Stoff oder die Aufnahme eines Nahrungsmittels haben gelegentlich unangenehme Folgen. Juckender Hautausschlag, tränende Augen, Durchfall oder sogar akuter Schockzustand können Zeichen einer allergischen Reaktion sein. Wenn so viele Menschen davon betroffen sind, lohnt es sich, dem Thema ein wenig auf den Grund zu gehen. Was ist eine Allergie überhaupt? Wie entsteht sie und wie kann man unerwünschte Begleiterscheinungen bekämpfen?

Einen prima Einstieg bietet wie bei vielen Themen Wikipedia. Der Eintrag unter de.wikipedia.org/wiki/Allergie verrät, dass der Wiener Kinderarzt Freiherr Clemens von Pirquet den Begriff Allergie im Jahre 1906 geprägt hat. Per Definition handelt es sich um eine „veränderte Fähigkeit des Körpers, auf eine fremde Substanz zu reagieren". Auch über mögliche Symptome klärt Wikipedia auf: Es gibt Reaktionen der Schleimhäute, der Atemwege, der Haut, des Verdauungstrakts und sogar akute Notfälle, die sich in einem anaphylaktischen Schock äußern.

Etwa 20 Prozent aller Deutschen leiden unter Heuschnupfen, einer allergische Reaktion auf Pollen. Die meisten reagieren nur auf einige wenige blühende Bäume, Sträucher, Gräser, Kräuter oder Getreidearten. Manche Allergiker leiden jedoch unter Pollenarten mit unterschiedlichen Blütezeiten und somit fast ganzjährig. Nachzulesen im Stern Ratgeber Allergie (www.stern.de/allergie/erkrankungen/585217.html), der eine schöne Fotogalerie mit Heuschnupfenauslösern mitliefert.

Um schon am Morgen abschätzen zu können, mit wie viel Schniefen und Augentränen der Tag verbunden sein wird, lohnt sich für Allergiker ein Blick in die Pollenflugvorhersage des Deutschen Wetterdienstes. Unter www.dwd.de/de/wir/Geschaeftsfelder/Medizin/Pollenvs/abfrage.htm lässt sich der Allergieauslöser auswählen, und eine Deutschlandkarte gibt einen Überblick über die Pollenflugintensität des Tages. Ebenfalls über diese Webseite kann man den Pollenflug-Newsletter des Wetterdienstes bestellen – somit flattert die Vorhersage des Tages pünktlich am Morgen ins E-Mail-Postfach.

Desensibilisierung per Tablette

Wer im wahrsten Sinne des Wortes die Nase voll hat vom Heuschnupfen, kann sich einer langwierigen Desensibilisierung unterziehen. In einem bis zu mehreren Jahren dauernden Prozess wird der Körper mithilfe von Spritzen oder Tropfen an den Allergieauslöser gewöhnt. Seit einiger Zeit gibt es alternativ eine Tablette, die ähnlich wirkt wie die seit langer Zeit bekannten Mittel, die ein Betroffener jedoch eigenständig zu Hause einnehmen kann. Mehr darüber weiß das WDR Fernsehen in seiner Aktuellen Stunde zu berichten: www.wdr.de/tv/aks/checkup/20070224_heuschnupfen.jhtml. Von dort aus geht es auch zu weiteren Webseiten rund um das Thema Heuschnupfen.

Ebenfalls in Deutschland weit verbreitet ist die Tierhaarallergie, ein leicht irreführender Begriff. Denn bei Katze, Kaninchen und Co. ist oftmals nicht das Fell an sich allergieauslösend, schuld sind stattdessen oder zusätzlich Bestandteile von Kot, Urin oder Hautschuppen. Es kommt häufig vor, dass Allergiker sich nicht mit dem reaktionsauslösenden Tier in einem Raum befinden können, ohne von Symptomen geplagt zu werden. Manchmal genügt es schon, auf offener Straße mit einem Katzenhalter ins Gespräch zu kommen, um heftige Reaktionen zu spüren. Besonders gemein ist, dass einige Tierallergene über große Distanzen schweben können – selbst in der Antarktis haben Forscher schon Katzenhaarallergene gefunden. Nachzulesen bei Gesundheit.de (www.gesundheit.de/krankheiten/allergie/tierhaarallergie/index.html) sowie im Onlineangebot des Stern (www.stern.de/allergie/erkrankungen/:Tierhaarallergie-Was-Haustiere-Plagegeistern/585228.html).

Schätzungsweise eine Million Deutsche leiden an einer Hausstauballergie. Oder besser gesagt, an einer Hausstaubmilbenallergie. Allergieauslöser sind nicht die Miniwesen selbst, sondern deren Kot, den sie in der Wohnung reichlich verteilen. Mit Freuden leben die Milben – die so klein sind, dass Hunderte von ihnen auf einen Stecknadelkopf passen – wo es warm und ein wenig feucht ist und wo sie sich von menschlichen Hautschuppen ernähren können. Richtig, die perfekten Lebensbedingungen findet sie in den Betten. Für die meisten Menschen ist dies kein Problem, doch sobald eine Allergie vorherrscht, kann der Aufenthalt in der eigenen Wohnung zur Qual werden. Wie gut, dass es unter www.enius.de/allergien/hausstauballergie.html viele Tipps zur Linderung gibt. Von der Bauanleitung für Do-it-Yourself-Allergikerbettwäsche bis hin zum Hinweis, dass man bei glatten Böden statt zum Staubsauger lieber zum Wischlappen greifen sollte – hier gibt es einige Ideen zum Ausprobieren. Wer keinen Ekel kennt, sollte zusätzlich einen Abstecher nach 82.198.66.21/Galerie.htm machen – die enorm vergrößerten Fotografien von Hausstaubmilben sind einen Blick wert.

Während umfangreiche Forschungen stattfinden, um weit verbreitete Allergien zu lindern, und man bereits etliche Medikamente zur Eindämmung der Symptome entwickelt hat, gibt es einige wenige Menschen, die unter wenig verbreiteten oder gar fast vollständig unerforschten Allergien leiden. Eine besonders seltene ist die Spermaallergie (de.wikipedia.org/wiki/Spermaallergie), die hauptsächlich zwanzig- bis dreißigjährige Frauen betrifft. Hierbei handelt

es sich um eine allergische Reaktion auf ein Protein im Ejakulat des Mannes, die sich durch Brennen, Juckreiz, Schwellungen oder Hausausschläge äußert. Das kann so weit gehen, dass bei einem Kinderwunsch kein Weg an der künstlichen Befruchtung vorbeiführt.

Wenig bekannt ist auch, dass für einige Menschen das Telefonieren mit dem Handy Hautausschläge hervorrufen kann, ausgelöst durch das in vielen Mobiltelefonen enthaltene Nickel (www.focus.de/gesundheit/ratgeber/allergie/news/nickel_aid_233441.html).

URLs auf einen Blick

de.wikipedia.org/wiki/Allergie
www.stern.de/allergie/erkrankungen/585217.html
www.dwd.de/de/wir/Geschaeftsfelder/Medizin/Pollenvs/abfrage.htm
www.wdr.de/tv/aks/checkup/20070224_heuschnupfen.jhtml
www.gesundheit.de/krankheiten/allergie/tierhaarallergie/index.html
www.stern.de/allergie/erkrankungen/:Tierhaarallergie-Was-Haustiere-Plagegeistern/585228.html
www.focus.de/gesundheit/ratgeber/allergie/news/nickel_aid_233441.html
www.vitanet.de/fitness-gesundheit/tipp-der-woche/ernaehrung/allergie-fisch
www.enius.de/allergien/hausstauballergie.html
82.198.66.21/Galerie.htm
de.wikipedia.org/wiki/Spermaallergie
www.bio-fuers-baby.de/allergien.php
www.allergien-behandeln.de/naet-therapie.html
www.gesundheit.de/forum/allergie

Wer weitere URLs zum Thema kennt, hat die Möglichkeit, sie der Online-Version (www.heise.de/ix/artikel/2008/04/152/) hinzuzufügen.

Vorbeugen beginnt im Mutterleib

Neuere Untersuchungen zeigen, dass werdende Mütter mit der richtigen Ernährung während der Schwangerschaft das Allergierisiko für ihr Kind senken können. Fisch beispielsweise wirkt sich mit seinen Omega-3-Fettsäuren positiv aus (www.vitanet.de/fitness-gesundheit/tipp-der-woche/ernaehrung/allergie-fisch). Doch Fisch ist nicht gleich Fisch – Sushi und Räucherlachs sind während der Schwangerschaft tabu. Vielleicht doch lieber durch Rapsöl ersetzen? Weitere Tipps, wie sich Allergien beim Kind eindämmen lassen, gibt es unter www.bio-fuers-baby.de/allergien.php.

Wer den Glauben an die Schulmedizin bereits verloren hat, kann sich vielleicht mit der Naet-Therapie (www.allergien-behandeln.de/naet-therapie.html) anfreunden, die mit einem ganzheitlichen Ansatz versucht, den Köper wieder ins Reine zu bringen. Oftmals reicht es jedoch schon aus, sich mit Leidensgenossen auszutauschen, dann ist man im Allergie-Forum (www.gesundheit.de/forum/allergie) genau richtig. Hier lassen sich Tipps und Tricks finden, die den Umgang mit der eigenen Allergie erleichtern. (ka)

Vor 10 Jahren: Als die Schwerkraft siegte

Nicht zum ersten Mal war Apple mit dem Newton der Zeit voraus. Durchsetzen konnte sich der Messagepad damals jedoch nicht.

Apple ist heute als Produzent von Geräten wie dem iPhone und den iPods bekannt, die schick aussehen und einfach zu bedienen sind. Zwei, drei Dinge können diese Geräte in der Regel wesentlich besser als vergleichbare Produkte der Konkurrenz. Hinzu kommt ein ordentliches Stück Marketing, das damit beginnt, dass Apple-Chef Steve Jobs neue Geräte in einer Kulthandlung vorführt. Vor 10 Jahren kam Jobs zu Apple (zurück) und stoppte die Produktion der Apple Messagepads. Über das Aus für diese als Apple Newton bekannt gewordenen Rechner, die ihrer Zeit weit voraus waren, berichtete *iX* in der Ausgabe 4/98. Damals wurde über die Produktionseinstellung viel gerätselt, heute kann man in den einschlägigen Jobs-Biografien die Gründe nachlesen: Der erste einigermaßen brauchbare Personal Digital Assistent (PDA) war das Lieblingsprojekt von John Sculley – und Jobs entfernte alles, was bei Apple an Sculley erinnerte.

Als Sculley 1987 (!) mit „Odyssey“ das Grundkonzept des später Newton genannten PDA beschrieb und seine Ingenieure daraufhin die Entwicklung eines Informations-Assistenten starteten, dachten sie überhaupt nicht an einen Pocket-Computer als Helferlein im digitalisierten Alltag. Die Vision war viel größer: Ein Knowledge Navigator sollte dem Menschen zur Hand gehen und dabei helfen, eine Informationsschicht als zweite Haut zu tragen. Schon der Projektname war alles andere als bescheiden: „Defying Gravity“ – der Schwerkraft trotzen, die Schwerkraft gar überwinden sollte das Informationssystem, worauf noch Newton OS, der Name des Betriebssytems hindeutete (Newton sitzt im allerersten Apple-Logo unter einem Baum, von dem ein Apfel fällt).

Sprach- und Handschriftenerkennung, Multimedia, komplett mit integriertem sprechenden Haus-Assistenten und einem Wissensreservoir, aus dem verschiedene Programme von der Terminplanung bis zum CAD schöpfen können: All das sollte den Knowledge Navigator auszeichnen. Für viel Geld drehte man einen Schulungsfilm über ihn, der heute zu den wichtigsten Zukunftsentwürfen der Branche gezählt wird im Verein mit dem Memex von Vannevar Bush (1945), der „Mother of all Demonstrations“ von Douglas Engelbart (1968) und der „You will“-Kampagne von AT&T (1993).

Was Bush auf Papier erklärte, was Engelbart seinem Publikum vor Ort erklären musste und was Sculleys Ingenieure noch per Video aufzeichneten, ist heute längst ins Internet gewandert. Viele Dinge, die der unzeitige Newton erstmals bot, benutzen die Besitzer aktueller Smartphones ganz selbstverständlich, von der Handschriftenerkennung über die Sprachsteuerung bis hin zum durchgehenden Datenkonzept für Terminkalender und Adressbuch. Wer heute die Konzepte der Zukunft sehen will, besucht Youtube oder einen anderen Videodienst und holt sich dort das „Morph“-Video von Nokia ab. Im Abspann des Trickfilms über die Wissensnavigation der Zukunft findet sich eine kleine Hommage – an den Newton natürlich. Die Schwerkraft konnte er nicht überwinden, aber im Gedächtnis der Informationsgesellschaft hat er seinen Ehrenplatz. Irgendwo in einer Wüste Nevadas soll es eine Newton-Müllhalde geben. Fans, die ihren PDA bis heute nutzen, suchen sie wie den heiligen Gral.

Detlef Borchers

MEHR KBYTES

Javascript

Jahrelang galt die Verwendung von Javascript auf Webservern fast als böse. Nicht allzu lange nach dem Anbruch des Ajax-Zeitalters (18. Februar 2005, mit Jesse James Garretts Aufsatz „Ajax: A New Approach to Web Applications“) hat sich die Situation geändert: Webentwickler müssen fit in dieser Sprache sein, denn ohne die Skriptsprache geht in Ajax-Anwendungen nichts. Autoren von Javascript-Büchern hat Asynchronous Javascript and XML Arbeit für neue Kapitel verschafft, denn seit 2006 darf kein JS-Buch mehr erscheinen, das nicht mindestens ein Kapitel zu diesem Umfeld enthält. Einige speziell Ajax gewidmete Bücher sind auf dieser Seite im April 2007 hoffentlich zu ihrem Recht gekommen, das eine oder andere haben *iX*-Autoren besprochen. Hier soll es um Javascript-Literatur gehen, die sich hauptsächlich der Sprache annimmt und Ajax nur unter anderem behandeln.



Schon Ende 2006 hat O’Reilly die zweite Auflage des von Nick Heinle, Bill Peña und Ulrich Speidel verantworteten „Webdesign mit JavaScript & Ajax“ in der Basics-Reihe veröffentlicht. Es handelt sich im Grunde um eine um zwei Kapitel erweiterte Javascript-Einführung, die ohne Ajax schon 2002 erschienen war. Wer’s knapp und/oder für unterwegs haben möchte, dem reichen unter Umständen die neuen 250 Seiten.

Ebenfalls schon 2006 erschienen ist die zweite Auflage des praktischen Javascript-Führers aus der No Starch Press, verfasst von Wired-Autor Thau. Der Band enthält, bei 470 Seiten Umfang nicht anders zu erwarten, deutlich mehr an Ajax-Material. Thau geht anders vor als das Gros der Autoren, indem er sich von vornherein mit dem auseinandersetzt, was Webentwickler „drückt“. Zwar beschreibt er anfangs, wie man Variablen und eingebaute Funktionen benutzt, aber vor allem will er dabei zeigen, wie Webseiten automatisch zu aktualisieren sind. Weitere Kapitel gehen ebenfalls problemorientiert vor: Rollovers, Öffnen und Schließen von Fenstern, wie man Frames und Image Maps einsetzt – und eben Ajax, von den Grundlagen bis zum Debugging.

Wohl das kürzeste Javascript-Buch ist das von Markus Nix herausgegebene „Exloring JavaScript“, erschienen bei der Entwickler-Press. Auf circa 160 Seiten lässt sich zwar keine umfassende Einführung unterbringen, aber Nix und seine Koautoren haben einen Überblick zusammengestellt, der erste Einblicke in Objektorientierung, Ajax und JSON (Javascript Object Notation) erlaubt. Wiederum gilt: keine stringente Einführung in die Sprache.

Wer das zuletzt Erwähnte will, benötigt schwergewichtige Bände, die selten unter 500 Seiten zu haben sind und vereinzelt die Tausendergrenze überschreiten. In diese Gruppe gehört Christian Wenz’ „JavaScript und Ajax“, das zwar seit der siebten Auflage nur um gute zehn Seiten gewachsen ist, insgesamt aber über 800 auf die Waage bringt. Hintergrund: Schon in der Vorauflage hat der Autor die Struktur erweitert, um Ajax integrieren zu können. Kapitel wie die zur Programmierung, Kommunikation oder Sicherheit dürften sich im Vergleich zu Auflage 7 deshalb kaum geändert haben; hinzugekommen sind Abschnitte zu Microsofts Ajax-Paket und Silverlight. Wie die beiden folgenden Bände eine seit Jahren erfolgreiche Einführung samt Referenz. Schmankerl: eine einstündige DVD mit Lernvideos.

David Flanagans in der Betaversion erstmals 1996 verlegte Javascript-Referenz, der Tausendseiter unter den hier vorgestellten, eignet sich schon deshalb definitiv nicht für mobile Programmierer (was für Wenz ebenfalls gilt). Im Original 2006 veröffentlicht (5. Auflage), liegt das Werk seit 2007 in deutscher Sprache vor. Ajax kommt in mehreren Kapiteln vor, steht aber nicht im Zentrum des Bandes, der vielmehr eine systematische Einführung in die Sprache bietet. Das allerdings ausführlich, bis hin zu Prototypen und Namensräumen.

Stefan Koch kommt in seiner bei dpunkt erschienenen Einführung mit weniger als 500 Seiten aus. Sein Buch hat sich ebenfalls schon eine Weile am Markt gehalten, die vierte Auflage ist komplett überarbeitet und enthält ein eigenes Ajax-Kapitel. Abgesehen davon bietet Koch den allmählichen Einstieg, indem er von Variablen über Verzweigungen und Schleifen zu komplizierteren Sprachaspekten wie Funktionen, Objekten und Arrays voranschreitet.

Wenz’, Flanagans sowie Kochs Werk enthalten jeweils eine Sprachreferenz. Eine Entscheidung zwischen den drei Bänden fällt schwer und dürfte, abgesehen von der Tragebereitschaft, vom Bedürfnis nach Struktur abhängen.

Head-First-Bücher (auf Deutsch „… von Kopf bis Fuß“) unterscheiden sich deutlich von den anderen. Das gilt auch für Michael Morrisons gerade erschienenen Javascript-Band, der wie die ganze Reihe eine Mischung aus gesetztem Text, handschriftlichen Zusätzen, Sprechblasen und Comic-Bildchen ist. Wie Koch hat Morrison ein eigenes Kapitel zu Ajax an den Schluss des Bandes gestellt. In diesem Fall dürfte die Entscheidung für oder gegen dies Buch nicht nur inhaltlich begründet sein. *Henning Behme*

David Flanagan; JavaScript; Das umfassende Referenzwerk; Sebastopol, CA (O’Reilly) 2007; übersetzt von Lars Schulten und Ulrich Speidel; deutsche Ausgabe der 5. Auflage; 1086 Seiten; € 54,90 (gebunden)

Nick Heinle, Bell Peña, Ulrich Speidel; Webdesign mit JavaScript & Ajax; Köln (O’Reilly) 2006; 2. Auflage; 254 Seiten; € 24,90 (Paperback)

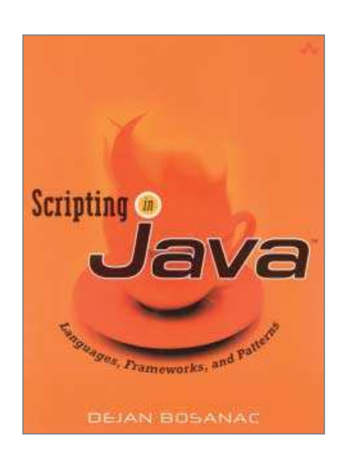
Stefan Koch; JavaScript; Einführung, Programmierung und Referenz; Heidelberg (dpunkt) 2007; 4., komplett überarbeitete Auflage; 436 Seiten; € 39,– (gebunden)

Michael Morrison; Head First JavaScript; Sebastopol, CA (O’Reilly Media) 2007; 615 Seiten; € 38,– (Paperback)

Markus Nix (Hrsg.); Exploring JavaScript; OOP, Ajax und Web 2.0; Frankfurt/Main (Software & Support) 2007; 165 Seiten; € 24,90 (Paperback)

Thau!; The Book of JavaScript; A Practical Guide to Interactive Web Pages; San Francisco, CA (No Starch Press) 2006; 490 Seiten; US-$ 39,95 (Paperback)

Christian Wenz; JavaScript und Ajax; Das umfassende Handbuch; Bonn (Galileo Computing) 2007; 853 Seiten zzgl. DVD; € 39,90 (gebunden)



Dejan Bosanac

Scripting in Java

Languages, Frameworks and Patterns

Upper Saddle River, NJ 2007
Addison-Wesley
528 Seiten
44,99 US-$
ISBN 978-0-321-32193-0

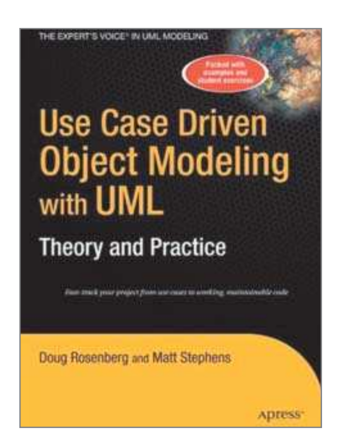
Nicht nur bei Unix-Kennern hat die Automatisierung wiederkehrender Tätigkeiten durch Scripts eine lange Tradition. Neben den vielen alten Bekannten (Perl, Tcl) buhlen zunehmend junge Sprachen mit ambitionierten Funktionen um die Gunst des Programmierers. In „Scripting in Java“ beleuchtet Dejan Bosanac dieses vielschichtige Thema aus der Sicht des Java-Entwicklers.

Die ersten beiden allgemein gehaltenen Kapitel definieren den Begriff der „Skriptsprache“ und stellen vorstellbare Einsatzgebiete vor. In seiner Abgrenzung zu klassischen Programmiersprachen greift der Autor den vom Tcl-Erfinder John Ousterhout geprägten Begriff der „system programming language“ und damit indirekt auch die nach Ousterhout benannte Dichotomie zwischen den Systemprogrammier- und den Skriptsprachen auf, die nicht zu Unrecht oft hinterfragt und kritisiert wurde. Das dritte Kapitel stellt einige Skriptsprachen vor, die in Javas virtueller Maschine ausgeführt werden. Der Leser lernt ihre wichtigen Funktionen kennen und erhält Tipps zu Installation und Zugriff.

Kapitel 5 und 6 widmet der Autor ausführlich Groovy. Hier begnügt er sich nicht mit der obligatorischen Aufzählung von Eigenschaften, sondern bietet eine recht gelungene Einführung in die Sprache. Dabei behandelt er auch anspruchsvolle Themen wie Datenbankzugriffe. Welche Vorteile und Erleichterungen der Einsatz von Skriptsprachen in der täglichen Arbeit bieten kann, zeigt der Autor in den beiden Kapiteln „Practical Scripting in Java“ und „Scripting Patterns“. Eines seiner Codebeispiele demonstriert den Einsatz von Groovy bei der Erstellung von Unit Tests.

Für den Zugriff auf Skriptsprachen setzt Bosanac oft, aber nicht durchgängig, das ursprünglich von IBM entwickelte, später an die Apache Software Foundation (ASF) übergebene „Bean Scripting Framework“ ein. Dessen Thronerbe, die im Java Specification Request 223 spezifizierte Scripting-API, die in Java Einzug in den Standard gefunden hat, findet ebenfalls eine gebührende Würdigung, wenngleich man sich eine gleichmäßigere Einbeziehung in die Beispiele des Buches wünschen würde. Trotzdem ist „Scripting in Java“ äußerst lesenswert. Die Lektüre macht Appetit, die Vorschläge des Autors in eigenen Projekten in die Tat umzusetzen.

THOMAS KÜNNETH



Doug Rosenberg, Matt Stephens

Use Case Driven Object Modeling with UML

Theory and Practice

Berkeley, CA 2007
APress
472 Seiten
54,99 US-$
ISBN 978-1-59059-774-3

Selten wird die schon im November 1997 standardisierte Unified Modeling Language (UML) in IT-Projekten wirklich als Sprache zur Verständigung über Anforderungen und als Stütze der gesamten Projektkommunikation genutzt. Offenbar ist es schwierig, die mannigfaltigen Optionen von 13 Diagrammtypen und den möglichen Beziehungen zwischen Artefakten theoretisch zu kennen. Erst recht, diese praktisch anzuwenden und sich damit und darüber in UML zu verständigen.

Von einzelnen UML-affinen Entwicklern erstellte Diagramme erleichtern aber weder die externe Kommunikation mit den Kunden noch erzeugen sie eine intersubjektive Nachvollziehbarkeit innerhalb des Projektteams. Sie verkomplizieren die Projektabwicklung unter Umständen mehr, als sie vereinfachen.

Im ihrem Buch „Use Case Driven Object Modeling with UML“ zeigen Doug Rosenberg und Matt Stephens, dass es auch anders geht. Das von ihnen propagierte ICONIX-Modell setzt UML für die Modellierung sogenannter Use Cases ein. Ergänzt um ein Domain-Glossar und „robustness diagrams“ zeigen sie für jede Phase eines Softwareprojekts theoretisch und praktisch, wie UML-Usecases sinnvoll und effizient genutzt werden können.

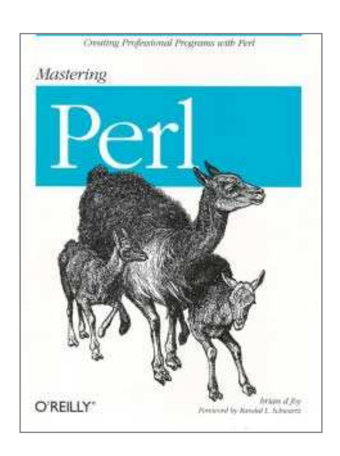
Der stringente und integrierte Ansatz überzeugt in theoretischer und praktischer Hinsicht, denn der erfahrungsreiche Hintergrund der Autoren ist durch das ganze Buch spürbar. Die praktische Umsetzung stellen die Autoren in der zweiten Hälfte mit einem konkreten Softwaretool, dem Enterprise Architect, vor.

Trotz der moderaten Kosten wird nicht jeder genau dieses Tool nutzen können oder dürfen. Die Übernahme der Grundgedanken in den eigenen Entwicklungskontext erleichtert jedenfalls die konkrete Darstellung.

Ob der ausgesparte Rest der UML-Spezifikation tatsächlich für die Praxis nicht sinnvoll nutzbar ist, wie die Autoren behaupten, und ob die im Buch formulierte deutlich Kritik an manchen agilen Entwicklungstechniken nicht durch eine nähere Betrachtung entschärft oder gar aufgelöst werden könnte, muss an dieser Stelle offen bleiben.

Wer schließlich wissen möchte, wie Entwickler die Modellierungssprache und Usecases im Rahmen eines durchgängig anforderungsbezogenen und erprobten Softwareerstellungsprozesses effizient nutzen können, dürfte mit diesem Buch voll auf seine Kosten kommen.

PETER EBENHOCH



Brian D. Foy

Mastering Perl

Sebastopol, CA 2007
O'Reilly Media, Inc.
342 Seiten
38,– €
ISBN 978-0-596-52724-2

Zum Teil schlampiger Einsatz von Perl vor allem im Webumfeld hat das Entstehen von Publikationen gefördert, die den sachgemäßen Gebrauch der Sprache thematisieren. In diese Kategorie fällt auch der Band „Mastering Perl“ von Brian D. Foy, dem Herausgeber der Zeitschrift „Perl Review“.

Das Buch behandelt Fragestellungen aus den drei großen Bereichen „fortgeschrittene Sprachmittel“, „Entwicklungswerkzeuge“ und „Standardaufgaben der Programmierung“. In den beiden letztgenannten Bereichen orientiert sich die Themenauswahl an den Bedürfnissen des Praktikers. Foy bietet insgesamt eine handwerklich solide Anleitung zum Lösen gängiger Aufgaben der Softwareentwicklung, nicht aber den im Vorwort versprochenen „way of thinking about Perl programming“. Diesbezüglich helfen auch nicht die wohlmeinenden Hinweise im Anhang. Die Kapitel sind zwar weitgehend unabhängig voneinander lesbar, ihre Anordnung folgt aber keinem offensichtlichen Prinzip, und sie schließen stets mit einer kurzen Zusammenfassung sowie nützlichen Literaturhinweisen. Die Quelltextbeispiele sind kurz und hilfreich, obwohl ihre Formatierung gewöhnungsbedürftig ist.

Nach dem ersten Kapitel, das die Rolle eines erweiterten Vorworts hat, erklärt der Autor die Feinheiten regulärer Ausdrücke und die Grundlagen sicherer Programmierung vor allem mit dem Taint-Modus. Es folgen drei Kapitel zu den verwandten Themen Debugging, Profiling und Benchmarking, in denen er die einschlägigen Standard-Werkzeuge vorstellt. Leider geht er auf die darunterliegende API nur am Rande ein.

Es schließt sich ein kurzes Kapitel zum Umgang mit Quelltexten an, auf das zwei gelungene Abschnitte zu Symboltabellen und anonymen Subroutinen folgen, einer Technik, die in den letzten Jahren zunehmend an Bedeutung gewonnen hat. Foy beschreibt danach, wie man in existierende Module eingreift, bevor er in zwei Kapiteln das Thema Fehlerbehandlung aufgreift. Er geht dabei auch auf Exceptions und die Protokollierung mit Log4perl ein. Es folgen Kapitel über Datenpersistenz, Programmdokumentation sowie das Arbeiten mit Bitvektoren, wobei Letzteres kein perlspezifisches Thema ist. Kapitel über mit *tie()* gebundene Variablen und Module als Programme schließen den Haupttext ab. Die Anhänge enthalten Literaturhinweise und die eingangs erwähnten Tipps zum Lösen von Programmierproblemen.

Foy bringt vieles und manchen etwas. Häufig geht er jedoch auf Details nicht ein, was er nicht zu Unrecht mit der Beschränkung der Seitenzahl entschuldigt. Insgesamt bringt der Band eine gelungene Mischung praxisrelevanter Themen für auf dem Weg zur Meisterschaft fortschreitende Perl-Entwickler.

DR. PETER DINTELMANN


MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Postfach 61 04 07, 30604 Hannover; Helstorfer Straße 7, 30625 Hannover

Redaktion
Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de
Abonnements: Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Herausgeber: Christian Heise, Ansgar Heise

Redaktion: Chefredakteur: Jürgen Seeger (JS) -386

Stellv. Chefredakteur: Henning Behme (hb) -374

Ltd. Redakt.: Kersten Auel (ka) -367, Ralph Hülsenbusch (rh) -373, Bert Ungerer (un) -368

Jürgen Diercks (jd) -379, Christian Kirsch (ck) -590, Wolfgang Möhle (WM) -384, Susanne Nolte (sun) -689, André von Raison (avr) -377, Michael Riepe (mr) -787, Ute Roos (ur) -535

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

Korrespondent Köln/Düsseldorf/Ruhrgebiet:
Achim Born, Siebengebirgsallee 82, 50939 Köln,Telefon: 02 21/4 20 02 62,
E-Mail: ab@ix.de

Korrespondentin München:
Susanne Franke, Ansbacherstr. 2, 80796 München, Telefon: 089/28 80 74 80,
E-Mail: sf@ix.de

Ständige Mitarbeiter: Torsten Beyer, Detlef Borchers, Fred Hantelmann, Kai König, Michael Kuschke, Barbara Lange, Stefan Mintert, Holger Schwichtenberg, Susanne Schwonbeck, Christian Segor, Diane Sieger, Axel Wilzopolski, Nikolai Zotow

DTP-Produktion: Enrico Eisert, Wiebke Preuß, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat/Chefin vom Dienst: Anja Fischer

Fotografie: Martin Klauss Fotografie, Despetal/Barfelde

Titelidee: ***iX;*** Titel- und Aufmachergestaltung: Dietmar Jokisch

Verlag und Anzeigenverwaltung:
Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Helstorfer Straße 7, 30625 Hannover; Telefon: 05 11/53 52-0, Fax: 05 11/53 52-129

Geschäftsführer: Ansgar Heise, Steven P. Steinkraus, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de

Assistenz: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigendisposition: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigenverkauf: PLZ-Gebiete 0–3, Ausland:
Oliver Kühn -395, E-Mail: oliver.kuehn@heise.de,
PLZ-Gebiete 8–9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de
Sonderprojekte: Isabelle Paeseler -205, E-Mail: isabelle.paeseler@heise.de

Anzeigen-Inlandsvertretung: PLZ-Gebiete 4–7:
Karl-Heinz Kremer GmbH, Sonnenstraße 2, D-66957 Hilst,
Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22, E-Mail: karlheinz.kremer@heise.de

Anzeigen-Auslandsvertretung:
Großbritannien, Irland: Oliver Smith & Partners Ltd. Colin Smith, 18 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX, UK, Telefon: (00 44) 20/79 78-14 40, Fax: (00 44) 20/79 78-15 50, E-Mail: colin@osp-uk.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 20 vom 1. Januar 2008.

Leiter Vertrieb und Marketing: Mark A. Cano (-299)

Werbeleitung: Julia Conrades (-156)

Teamleitung Herstellung: Bianca Nagel (-456)

Druck: Dierichs Druck + Media GmbH & Co. KG, Kassel

Sonderdruck-Service: Ruth Utesch (-359, Fax: -360)

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

***iX* erscheint monatlich**

Einzelpreis € 5,50, Österreich € 6,20, Schweiz CHF 10,70, Benelux € 6,70, Italien € 6,70

Das Abonnement für 12 Ausgaben kostet: Inland € 56,–, Ausland (außer Schweiz) € 63,–; Studentenabonnement: Inland € 42,–, Ausland (außer Schweiz) € 47,– nur gegen Vorlage der Studienbescheinigung (inkl. Versandkosten Inland € 8,30, Ausland € 13,30), Luftpost auf Anfrage.

iX-Abo+ (inkl. jährlicher Archiv-CD-ROM) jeweils zzgl. € 8,–

Für GI-, VDI-KfIT-, GUUG-, IUG-, LUG-, AUGE- und Mac-e.V.-Mitglieder gilt der Preis des Studentenabonnements (gegen Mitgliedsausweis).

Kundenkonto in Österreich:
Dresdner Bank AG, BLZ 19675, Kto.-Nr. 2001-226-00 EUR, SWIFT: DRES AT WX

Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0

Abo-Service:
Heise Zeitschriften Verlag, Kundenservice, Postfach 810520, 70522 Stuttgart,
Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Für Abonnenten in der Schweiz Bestellung über:
Thali AG, Aboservice, Industriestr. 14, CH-6285 Hitzkirch,
Telefon: 041/919 66 11, Fax: 041/919 66 77, E-Mail: abo@thali.ch, Internet: www.thali.ch (Jahresabonnement: CHF 111,–; Studentenabonnement: CHF 83,25)

Das Abonnement ohne Archiv-CD-ROM ist jederzeit mit Wirkung zur jeweils übernächsten Ausgabe kündbar. Das *iX-Abo+* (incl. jährlicher Archiv-CD-ROM) gilt zunächst für ein Jahr und ist danach zur jeweils übernächsten Ausgabe kündbar.

Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz): MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Str. 5, 85386 Eching, Telefon: 089/319 06-0, Fax: 089/319 06-113, E-Mail: mzv@mzv.de, Internet: www.mzv.de

Printed in Germany

ISSN 0935-9680





Open-Source-DMS für Mittelständler

Jedes Unternehmen muss Unmengen an Geschäftsunterlagen revisionssicher und über einen langen Zeitraum archivieren. Professionelle Dokumentenmanagement-software kostet in der Regel viel Geld, und quelloffene Angebote gibt es bislang kaum. Main Pyrus DMS steht unter der GPL und ist damit eine der wenigen Ausnahmen. Das Produkt besitzt einen klaren Archivierungsschwerpunkt und richtet sich vor allem an mittelständische Unternehmen.



Rundum-sorglos-Pakete für KMU

Für die zentrale Server-Infrastruktur greifen vor allen kleinere und mittlere Unternehmen mangels entsprechenden Know-hows oder beschränkter personeller Ressourcen der IT-Abteilung gern zu Komplettpaketen. Inzwischen tummeln sich in diesem Segment eine Reihe Linux-basierter Produkte, die Microsofts Small Business Server das Revier streitig machen wollen. *iX* stellt einige dieser Linux-Pakete dem Platzhirsch gegenüber und zeigt in einer Übersicht, welche Groupware-Lösungen im Markt für KMU zu finden sind.

Heft 05/2008 erscheint am 17. April 2008

Streitkultur in Onlineforen

Mailinglisten und Usenet/Newsgroups waren zu Beginn der 80er-Jahre der Ursprung technisch unterstützter Diskussionsplattformen. Im Zeitalter des Web (2.0) übernehmen Forensysteme diese Aufgabe. An der Netiquette hat sich kaum etwas geändert: Die Streitkultur, über Jahrzehnte gewachsen, wird weiter gepflegt. Am Beispiel von neun Produkten – überwiegend Open Source – offenbart sich das Spektrum der recht konservativ gestalteten Forensoftware.



CMS für die Community

Seit ein, zwei Jahren wird das Content-Management-System Drupal in der Diskussion um das bessere Open-Source-CMS häufiger genannt. Mit der Version 6 des vor allem aufs Social Web ausgerichteten Systems haben die Entwickler an der Erweiterbarkeit, Internationalisierung und Bedienung gearbeitet.

Umgangssprachliche Schnittstellen

Klare Strukturen, die unter anderem durch den Einsatz von Entwurfsmustern entstehen, helfen den Überblick in Projekten zu bewahren. Idealerweise sind auch die Programme selbst gut lesbar. Die Kombination des Builder Pattern mit einem sogenannten Fluent Interface erleichtert die Definition verständlicher Schnittstellen.

Das bringen





Mobil surfen: Seit dem iPhone ist alles anders

CPU-Überblick: Welcher x86-Prozessor für wen

Allround-Router in Konkurrenz zum Server-PC

Flash-Kartenleser: Welche sind wirklich schnell?

Heft 07/08 jetzt am Kiosk





Auf ins All: Warum private Raumfahrt ein spannender neuer Markt wird.

Spam als Geschäft: Organisierte Kriminelle unterwandern das Internet.

Bio, nicht Öko: Die deutsche Energiepolitik steckt voller Ungereimtheiten.

Heft 04/08 jetzt am Kiosk

TELEPOLIS

MAGAZIN DER NETZKULTUR



Frank Magdans: Point-and-Click, quo vadis?

Tom Appleton: Wittgenstein und Hitler? – Hinweis auf ein vergessenes Buch

www.heise.de/tp/